U d'/ of Ottawa
39003006860026

Digitized by the Internet Archive
in 2012 with funding from
University of Toronto

http://archive.org/details/thoriedesnombres02krai

Cornelius Gouwens.

See Corrections
Bulletin Nov Dec 1929

THÉORIE DES NOMBRES

PAR

M. KRAITCHIK

Ingénieur à la Société Financière de Transports et d'Entreprises Industrielles
Agrégé à l'Université de Bruxelles

TOME II

ANALYSE INDÉTERMINÉE DU SECOND DEGRÉ ET FACTORISATION

UNIVERSITAS SCIENTIAE OTTAVIENSIS

PARIS
GAUTHIER-VILLARS ET Cie, ÉDITEURS
55, Quai des Grands Augustins

1926

QA
241
.K73T2
1926

Ouvrage publié avec l'appui
de la
Fondation Universitaire Belge

AVANT-PROPOS.

Le présent volume fait suite à celui que nous avons publié en 1922. Il complète, en même temps, notre autre publication : *Recherches sur la théorie des nombres*, parue en 1924.

Nous avons examiné, dans ce volume, certaines questions qui se rapportent à l'équation indéterminée du second degré, ainsi qu'à l'étude des formes. Nous avons fait une étude arithmétique des formes, à laquelle, d'après la table des matières, la deuxième partie seule semble consacrée, mais, en réalité, dans plusieurs pages de la troisième partie, nous revenons sur cette question.

L'exposé de la théorie des formes et de certaines équations indéterminées, nous a conduit à commencer par un aperçu aussi concis que possible des fractions continues qui, depuis longtemps, sont connues dès les classes supérieures de l'enseignement secondaire.

Toutefois, nous avons consacré tout un chapitre (Chapitre III) à l'étude du développement de $\sqrt{A}$ pour toutes les valeurs de A inférieures à 1000.

Ce n'est pas tant les développements particuliers que nous avions en vue, mais les formules générales dont le degré d'indétermination est parfois très élevé.

Parmi ces formules générales, les plus intéressantes sont celles qui dépendent d'un seul paramètre.

Leur intérêt réside dans la possibilité de généraliser certaines questions qui dépendent de l'équation indéterminée du second degré à coefficients non numériques, ou dans l'étude des formes d'une certaine généralité (par exemple, des formes indéfinies, dont les coefficients sont certaines fonctions linéaires ou quadratiques). Toutefois, nous avons passé sous silence ces recherches spéciales afin de réduire les dimensions du présent ouvrage qui ont déjà dépassé celles que nous lui avions assignées.

La question de factorisation, que Gauss considérait avec raison comme *fondamentale*, est traitée dans notre ouvrage avec une

abondance de détails qu'on ne trouve pas habituellement dans un livre d'étude, et certaines notions y sont développées pour la première fois.

Il ne nous appartient pas de nous prononcer sur la valeur scientifique de notre exposé, mais nous avons la conviction de n'avoir épargné, ni notre travail, ni notre temps, pour élucider cette question importante.

La moitié de ce volume (3e partie) est consacrée à ce sujet.

C'est à cause de l'importance que nous attachons à cette question que nous avons mis en sous-titre « Analyse indéterminée du second degré et factorisation », bien qu'il ne soit pas nécessaire de répéter ce dernier mot, car, par les procédés que nous étudions, la factorisation se ramène à la résolution d'une équation indéterminée du second degré.

Il nous reste à remplir un bien agréable devoir en adressant nos vifs remercîments à la Fondation Universitaire qui a pris la généreuse initiative d'intervenir pécuniairement, ce qui a permis la publication de notre travail, malgré les conditions économiques pénibles que nous subissons.

Nous devons également remercier MM. de la Vallée Poussin et Demoulin, qui ont bien voulu nous aider de leurs précieux conseils pour la rédaction de cet ouvrage.

Si nous avons réussi à intéresser le lecteur à nos recherches, nous serons hautement récompensé de l'effort que nous nous sommes imposé.

Bruxelles, le 21 juillet 1926.
M. KRAITCHIK.

ABRÉVIATIONS

employées dans les références bibliographiques pour les autres travaux de l'auteur.

T. I. Théorie des nombres, Tome I, Paris 1922.

T. II. » » » II, » 1926.

R. Recherches sur la théorie des nombres, Paris 1924.

PREMIÈRE PARTIE.

Équations indéterminées du second degré à deux inconnues.

CHAPITRE PREMIER.

Des fractions continues.

1. Soit x une quantité positive rationnelle ou irrationnelle et posons

$$x = a_1 + \frac{1}{x_1}, \quad x_1 = a_2 + \frac{1}{x_2}, \quad \ldots, \quad x_{k-1} = a_k + \frac{1}{x_k}, \quad \ldots, \qquad (1)$$

a_k étant le plus grand nombre entier compris dans x_{k-1} ($k = 1, 2, 3, \ldots$).

Si on élimine $x_1, x_2, x_3, \ldots, x_k$, il vient

$$x = a_1 + \frac{1}{a_2} + \frac{1}{a_3} + \cdots + \frac{1}{a_{k-1}} + \frac{1}{a_k} + \cdots.$$

C'est ce qu'on nomme fraction continue arithmétique, seule que nous aurons à considérer. Nous la représenterons par la notation

$$x = a_1, a_2, a_3, \ldots, a_k, \ldots. \qquad (2)$$

Les nombres entiers a_k ($k = 1, 2, 3, \ldots$) sont positifs et s'appellent *quotients incomplets*. Le premier a_1 peut être nul si ($x < 1$) mais tous les autres sont $\geqslant 1$. Le dernier est généralement $\geqslant 2$, car si (2) est une fraction continue limitée, et si le dernier quotient incomplet est $a_k = 1$, on peut remplacer le précédent a_{k-1} par $a_{k-1} + \frac{1}{1} = a_{k-1} + 1$ et la fraction continue finit un terme avant qu'on ne le suppose.

Toutefois, dans certains cas, pour pouvoir disposer de la parité du rang du dernier quotient incomplet on fait le contraire et on remplace, si cela est nécessaire, a_k par $(a_k - 1) + \frac{1}{1}$.

Si x est une quantité rationnelle, l'une des quantités x_k est un entier et la suivante $x_{k+1} = \infty$. En effet, soit $x = \frac{A}{B}$ cette quantité rationnelle, A et B étant supposés premièrs entre eux. Si on exécute sur A et B les opérations du plus grand commun diviseur $A = Bq_1 + r_1$, $B = r_1 q_2 + r_2$, ..., $r_{k-1} = r_k\, q_{k+1} + r_{k+1}$ d'où ($r_{k+1} = 1$) on aura $\frac{A}{B} = q_1, q_2, q_3, \ldots, r_k$.

Mais si x est une quantité irrationnelle, aucune des quantités x_k n'est rationnelle ni à fortiori entière et la suite des quotients complets ou incomplets est indéfinie. En effet, si une des quantités x_k était rationnelle, toutes les précédentes le seraient aussi et x serait une quantité rationnelle.

On appelle *réduites* successives d'une fraction continue, les fractions qu'on obtient en arrêtant le développement de la fraction continue donnée au premier, deuxième, troisième, etc., quotient incomplet.

On démontrera facilement que tout nombre entier ou fractionnaire, rationnel ou irrationnel, est d'une seule façon égale à une fraction continue.

2. *Calcul des réduites.* — Soit

$$\frac{p_k}{q_k} \text{ la } k^{\text{ième}} \text{ réduite } (k = 1, 2, 3, \ldots).$$

Les termes des réduites successives se calculent par les formules de récurrence

$$\left.\begin{aligned} p_n &= p_{n-1}\, a_n + p_{n-2}, \\ q_n &= q_{n-1}\, a_n + q_{n-2}. \end{aligned}\right\} \quad (3)$$

En effet, ces formules étant supposées vraies pour la $n^{\text{ième}}$ réduite, on trouvera la réduite suivante en remplaçant dans

$$\frac{p_n}{q_n} = \frac{p_{n-1}a_n + p_{n-2}}{q_{n-1}a_n + q_{n-2}},$$

a_n par $a_n + \frac{1}{a_{n+1}}$. On trouve

$$\frac{q_{n+1}}{p_{n+1}} = \frac{p_{n-1}\left(a_n + \frac{1}{a_{n+1}}\right) + p_{n-2}}{q_{n-1}\left(a_n + \frac{1}{a_{n+1}}\right) + q_{n-2}} = \frac{p_n a_{n+1} + p_{n-1}}{q_n a_{n+1} + q_{n-1}}.$$

Or, les formules (3) se vérifient directement pour la troisième réduite, donc ces formules sont générales.

Corollaires. — 1° Les termes des suites récurrentes (R, p. 73) sont dans certains cas, les termes des réduites successives.

Ainsi, si $q = -1$, on aura

$$u_{n+1} = pu_n + u_{n-1}, \qquad v_{n+1} = pv_n + v_{n-1}.$$

Avec $p = 1$ on trouve la série de Fibonacci dont les termes sont ceux des réduites de la fraction

$$x = 0, 1, 1, 1, 1, 1, \ldots.$$

2° Si on introduit deux réduites fictives

$$\frac{p_{-1}}{q_{-1}} = \frac{0}{1}, \qquad \frac{p_0}{q_0} = \frac{1}{0},$$

on peut commencer le calcul des réduites par les formules de récurrence (3) dès la première réduite.

On trouve ainsi

		a_1	a_2	a_3		a_k	
0	1	a_1	$a_1a_2 + 1$	$(a_1a_2 + 1)\,a_3 + a_1$	$\cdots$	p_k	$\cdots$
1	0	1	a_2	$a_2a_3 + 1$	$\cdots$	q_k	$\cdots$

Dans la première ligne horizontale s'inscrivent les quotients incomplets successifs, dans la deuxième les numérateurs et dans la troisième les dénominateurs des réduites successives.

3. *Propriété des réduites.*— Entre les termes des deux réduites successives, on a la relation

$$p_nq_{n+1} - q_np_{n+1} = (-1)^n. \tag{4}$$

En effet, d'après les formules (3) il vient

$$p_nq_{n+1} - q_np_{n+1} = p_n(q_na_{n+1} + q_{n-1}) - q_n(p_na_{n+1} + p_{n-1})$$
$$= -(p_{n-1}q_n - q_{n-1}p_n).$$

Ainsi donc la quantité $\rho = (-1)^n(p_nq_{n+1} - q_np_{n+1})$ est une constante.

Pour déterminer cette constante, faisons $n = 1$, ce qui donne

$$\rho = (-1)[a_1 a_2 - (a_1 a_2 + 1)] = +1 = (-1)^n (p_n q_{n+1} - q_n p_{n+1}),$$

d'où
$$p_n q_{n+1} - q_n p_{n+1} = (-1)^n.$$

Corollaires. — 1° Les réduites sont des fractions irréductibles.

2° Les réduites de rang pair sont plus grandes que celles de rang impair.

3° La différence de deux réduites consécutives est

$$\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}} = \frac{(-1)^n}{q_n q_{n+1}}.$$

4° Les numérateurs (ainsi que les dénominateurs) de deux réduites successives sont premiers entre eux.

4. Soit
$$x = a_1, a_2, a_3, \ldots, a_k, \ldots,$$

une fraction continue et $\frac{p_k}{q_k}$ $(k = 1, 2, 3, \ldots)$ les réduites successives. Le valeur de x est toujours comprise entre deux réduites successives et chaque réduite approche plus de x que la précédente.

En effet, si dans

$$\frac{p_{n+1}}{q_{a+1}} = \frac{p_n a_{n+1} + p_{n-1}}{q_n a_{n+1} + q_{n-1}}.$$

on remplace le quotient incomplet a_{n+1} par le quotient complet

$$x_{n+1} = a_{n+1}, a_{n+2}, a_{n+3}, \ldots,$$

on trouve

$$x = \frac{p_n x_{n+1} + p_{n-1}}{q_n x_{n+1} + q_{n-1}},$$

d'où
$$q_n x_{n+1}\left(x - \frac{p_n}{q_n}\right) = q_{n-1}\left(\frac{p_{n-1}}{q_{n-1}} - x\right),$$

il résulte de la dernière égalité que les différences $x - \frac{p_n}{q_n}$ et $\frac{p_{n-1}}{q_{n-1}} - x$ sont de même signe, c'est-à-dire que

$$\frac{p_{n-1}}{q_{n-1}} < x < \frac{p_n}{q_n} \text{ si } n \text{ est paîr}$$

ou
$$\frac{p_{n-1}}{q_{n-1}} > x > \frac{p_n}{q_n} \text{ si } n \text{ est impair.}$$

De plus puisque $q_n x_{n+1} > q_{n-1}$, on aura en valeur absolue

$$\left| x - \frac{p_n}{q_n} \right| < \left| \frac{p_{n-1}}{q_{n-1}} - x \right|.$$

Corollaires. — 1° $\frac{p_k}{q_k}$ $(k = 1, 2, 3, \ldots)$ étant les réduites successives de x, on aura

$$\frac{p_1}{q_1} < \frac{p_3}{q_3} < \frac{p_5}{q_5} \ldots < \frac{p_{2n+1}}{q_{2n+1}} \ldots < x,$$

$$\frac{p_2}{q_2} > \frac{p_4}{q_4} > \frac{p_6}{q_6} \ldots > \frac{p_{2n}}{q_{2n}} \ldots > x.$$

2° Toute réduite est comprise entre deux réduites consécutives précédentes.

3° Quelles que soient k et l, on a

$$\frac{p_{2k+1}}{q_{2k+1}} < x < \frac{p_{2l}}{q_{2l}}.$$

4° Lorsque trois nombres positifs rangés par ordre de grandeur sont développés en fraction continue, les premiers quotients incomplets qui sont communs aux nombres extrêmes, sont aussi les premiers quotients incomplets du nombre de milieu, et les quotients qui complètent les trois fractions sont rangés par ordre de grandeur (dans le même ordre ou dans l'ordre inverse).

5. Soit ε la différence entre la valeur d'une fraction continue et la $n^{ième}$ réduite

$$(n = 1, 2, 3, \ldots), \qquad \varepsilon = x - \frac{p_n}{q_n}.$$

On aura en valeur absolue

$$\varepsilon < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n (q_n + q_{n-1})} < \frac{1}{q_n^2}.$$

En effet, x étant compris entre $\frac{p_n}{q_n}$ et $\frac{p_{n+1}}{q_{n+1}}$, on a en valeur absolue

$$\left| x - \frac{p_n}{q_n} \right| < \left| \frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}} \right|, \qquad \text{ou} \qquad \varepsilon < \frac{1}{q_n q_{n+1}}.$$

Ensuite $$q_{n+1} = q_n a_{n+1} + q_{n-1},$$

donne $$q_{n+1} \geqslant q_n + q_{n-1} > q_n,$$

ce qui donne les autres inégalités.

Corollaires. — 1° On a en valeur absolue

$$\frac{1}{q_n(q_n + q_{n+1})} < \left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}.$$

2° Si $x = a_1, a_2, a_3, \ldots$, et $\frac{p_n}{q_n}$ les réduites successives, on aura

$$x = a_1 + \frac{1}{q_1 q_2} - \frac{1}{q_2 q_3} + \frac{1}{q_3 q_4} \cdots + \frac{(-1)^n}{q_{n-1} q_n}.$$

3° On peut écrire $\left| x - \frac{p_n}{q_n} \right| = \frac{\delta}{q_n^2}$, δ étant inférieure à 1.

4° Étant donnée une fraction $\frac{p}{q}$ dont la différence avec une quantité x est $\pm \frac{\delta}{q^2}$, $(\delta < 1)$, la condition nécessaire et suffisante pour $\frac{p}{q}$ soit l'une des réduites du développement de x en fraction continue est $\delta < \frac{q}{q + q'}$, q' étant le dénominateur de la réduite qui précède $\frac{p}{q}$.

5° Si on a $p^2 - Aq^2 = \pm D$ avec $D < \sqrt{A}$, la fraction $\frac{p}{q}$ est une des réduites du développement de $\sqrt{A}$.

En effet, de l'équation donnée on tire

$$p - q\sqrt{A} = \frac{\pm D}{p + q\sqrt{A}}, \quad \text{ou} \quad \frac{p}{q} - \sqrt{A} = \frac{\pm D}{q(p + q\sqrt{A})}.$$

Soit $\frac{\pm \delta}{q^2}$ la différence $\frac{p}{q} - \sqrt{A}$, ou $\delta = \frac{Dq}{p + q\sqrt{A}}$.

Soit $\frac{p'}{q'}$ la réduite qui précède $\frac{p}{q}$ et qui sera choisie de façon à ce que δ ait le même signe que D.

On aura $\delta = \frac{Dq}{p + q\sqrt{A}}$. Il suffit de prouver qu'on peut avoir

$$\delta < \frac{q}{q + q'}, \qquad \text{ou} \qquad \frac{Dq}{p + q\sqrt{A}} < \frac{q}{q + q'},$$

ou $D(q + q') < p + q\sqrt{A}$, ou en remplaçant p par $q\sqrt{A} \pm \frac{\delta}{q}$

$(\sqrt{A} - D)(q + q') + (q - q')\sqrt{A} \pm \frac{\delta}{q} > 0$, ce qui est manifeste.

6. Théorème. — Si une fraction irréductible $\frac{p}{q}$ est comprise entre deux réduites successives $\frac{p_n}{q_n}$ et $\frac{p_{n+1}}{q_{n+1}}$, on aura $q > q_{n+1} > q_n$.

En effet, les différences $\frac{p}{q} - \frac{p_n}{q_n}$ et $\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}$ sont de même signe, et en valeur absolue la première est plus petite, on aura donc

$$\frac{p}{q} - \frac{p_n}{q_n} < \frac{1}{q_n q_{n+1}}, \qquad \text{ou} \qquad pq_n - qp_n < \frac{q}{q_{n+1}}.$$

Le premier membre étant entier et par hypothèse différent de zéro, le second l'est aussi, donc $q > q_{n+1}$.

Corollaire. — Chaque réduite d'une fraction continue approche plus de la valeur de x que toute autre fraction dont les termes sont moindres que ceux de la réduite.

7. *Fraction continue symétrique.* — Considérons la fraction continue

$$x = a_1, a_2, a_3, \ldots, a_n$$

et soit $\frac{p_1}{p_1}, \frac{p_2}{q_2}, \ldots, \frac{p_n}{q_n}$ les réduites successives.

On a

$$p_n = p_{n-1} a_n + p_{n-2}, \qquad \text{d'où} \qquad \frac{p_n}{p_{n-1}} = a_n + \frac{1}{p_{n-1} : p_{n-2}},$$

$$p_{n-1} = p_{n-2} a_{n-1} + p_{n-3}, \qquad \frac{p_{n-1}}{p_{n-2}} = a_{n-1} + \frac{1}{p_{n-2} : p_{n-3}},$$

. . . . . .

$$p_3 = p_2\, a_3 + p_1, \qquad \frac{p_3}{p_2} = a_3 + \frac{1}{p_2 : p_1},$$

$$p_2 = p_1\, a_2 + 1. \qquad \frac{p_2}{p_1} = a_2 + \frac{1}{p_1}.$$

On aura ainsi

$$\frac{p_n}{p_{n-1}} = a_n\,,\, a_{n-1},\, a_{n-2},\, \ldots,\, a_2,\, a_2,\, a_1.$$

On trouvera de même

$$\frac{q_n}{q_{n-1}} = a_n,\, a_{n-1},\, a_{n-2},\, \ldots,\, a_3,\, a_2.$$

Si donc $q_n = p_{n-1}$, on aura

$$\frac{p_n}{q_n} = a_1,\, a_2,\, a_3,\, \ldots,\, a_n\,,$$

$$\frac{p_n}{p_{n-1}} = a_n\,,\, a_{n-1},\, a_{n-2},\, \ldots,\, a_2,\, a_3,\, a_1 = \frac{p_n}{q_n}.$$

Ainsi pour que les deux développements

$$a_1,\, a_2,\, a_3,\, \ldots,\, a_n \qquad \text{et} \qquad a_n\,,\, a_{n-1},\, \ldots,\, a_3,\, a_2,\, a_1,$$

soient identiques il faut que le développement de $\frac{p_n}{q_n}$ soit symétrique.

Dans ce cas (4) devient

$$p_n\, q_{n-1} - q_n^2 = (-1)^n, \qquad \text{ou} \qquad q_{n-1} = \frac{q_n^2 + (-1)^n}{p_n}.$$

Réciproquement, si $\frac{p_n}{q_n}$ est une fraction irréductible et si p_n divise $q_n^2 \pm 1$, le développement de $\frac{p_n}{q_n}$ en fraction continue, donne une suite symétrique des quotients incomplets.

8. Cherchons quelle est la condition pour que deux irrationnelles x et y soient terminées par les mêmes quotients complets.

S'il en est ainsi, on aura

$$x = \frac{p_n\, x_{n+1} + p_{n-1}}{q_n\, x_{n+1} + q_{n-1}}, \quad y = \frac{p'_m\, y_{m+1} + p'_{m+1}}{q'_m\, y_{m+1} + q'_{m+1}} \quad \text{avec } x_{n+1} = y_{m+1},$$

ce qui donne

$$\frac{q_{n-1}\,x - p_{n-1}}{p_n - q_n\,x} = \frac{q_{m-1}\,y - p_{m-1}}{p_m - q_m\,y},$$

d'où

$$y = \frac{(q_{n-1}\,p'_m - p'_{m-1}\,q_n)\,x + (p_n\,p'_{m-1} - p'_m\,p_{n-1})}{(q_{n-1}\,q'_m - q'_{m-1}\,q_n)\,x + (p_n\,q'_{m-1} - q'_m\,p_{n-1})}.$$

Cette relation est de la forme $y = \dfrac{ax+b}{cx+d}$.

La quantité $ad - bc$ est

$$(q_{n-1}\,p'_m - p'_{m-1}\,q_n)(p_n\,q'_{m-1} - q'_m\,p_{n-1}) - (q_{n-1}\,q'_m$$
$$- q'_{m-1}\,q_n)(p_n\,p'_{m-1} - p'_m\,p_{n-1}) = p_n\,q_{n-1}\,p'_m\,q'_{m-1}$$
$$+ p_{n-1}\,q_n\,p'_{m-1}\,q'_m - p_n\,q_{n-1}\,p'_{m-1}\,q'_m - p_{n-1}\,q_n\,p'_m\,q'_{m-1}$$
$$= (p_n\,q_{n-1} - q_n\,p_{n-1})(p'_m\,q'_{m-1} - q'_m\,p'_{m-1}) = (-1)^{m+n}.$$

Ainsi la condition cherchée est qu'il existe entre x et y une relation de la forme

$$y = \frac{ax+b}{cx+d} \qquad \text{avec} \qquad \begin{vmatrix} a & b \\ c & d \end{vmatrix} = \pm 1.$$

On démontre facilement que cette condition est suffisante, c'est-à-dire que si x et y sont telles que

$$y = \frac{ax+b}{cx+d} \qquad \text{avec} \qquad \begin{vmatrix} a & b \\ c & d \end{vmatrix} = \pm 1,$$

les deux irrationnelles x et y se terminent par les mêmes quotients complets.

9. Soit $x = \dfrac{\sqrt{A} + N}{D}$ un nombre algébrique de second degré, c'est-à-dire racine d'une équation de second degré (A n'étant pas carré parfait) et cherchons le développement de x en fraction continue.

Posons $x = a_1 + \dfrac{1}{x_1}$, a_1 étant le plus grand nombre entier contenu dans x. On aura

$$x_1 = \frac{D_1}{\sqrt{A} - (a_1 D - N)}.$$

Afin de rendre le dénominateur rationnel, on multipliera les deux termes par $\sqrt{A} + (a_1 D - N)$ et on aura

$$x_1 = \frac{\sqrt{A} + N_1}{D_1} = a_2 + \frac{1}{x_2}.$$

On trouvera de même pour x_2 une expression de la forme

$$x_2 = \frac{\sqrt{A} + N_3}{D_3} = a_3 + \frac{1}{x_3},$$

et d'une façon générale

$$x_n = \frac{\sqrt{A} + N_n}{D_n} = a_{n+1} + \frac{1}{x_{n+1}}.$$

Nous allons démontrer que si N et D sont des nombres entiers toutes les qantités N_k, D_k le sont aussi.

Soit

$$x_n = \frac{\sqrt{A} + N_n}{D_n} = a_{n+1} + \frac{1}{x_{n+1}},$$

$$x_{n+1} = \frac{D_n}{\sqrt{A} - (a_{n+1} D_n - N_n)} = \frac{\sqrt{A} + N_{n+1}}{D_{n+1}}.$$

Il en résulte

$$\left.\begin{aligned} D_n D_{n+1} &= A - N_{n+1} (a_{n+1} D_n - N_n, \\ N_{n+1} &= a_{n+1} D_n - N_n. \end{aligned}\right\} \quad (5)$$

La deuxième formule (5) prouve que N_{n+1} est entier si N_n et D_n sont entiers.

La prémière formule (5) donne

$$D_n D_{n+1} = A - N_{n+1}^2, \qquad \text{ou} \qquad A = D_n D_{n+1} + N_{n+1}^2.$$

Ainsi donc la quantité $D_n D_{n+1} + N_n^2$, est constante, donc

$$D_n D_{n+1} + N_{n+1}^2 = D_{n+1} D_n + N_n^2,$$

ou $$D_n D_{n+1} + (a_{n+1} D_n - N_n)^2 = D_{n-1} D_n + N_n^2,$$

ou enfin $$D_{n+1} = -(a_{n+2}^2 D_n - 2a_{n+1} N_n - D_{n-1}). \quad (6)$$

Il en résulte que D_{n+1} est aussi un nombre entier dans les conditions envisagées.

Corollaires. — 1° Si D est pair et N impair, tous les D et tous les N seront de même parité.

2° D_n, N_{n+1} et D_{n+1} ne peuvent avoir aucun diviseur commun supérieur à 1.

10. Théorème. — Le développement d'un nombre rationnel du deuxième degré est une fraction continue périodique, c'est-à-dire que la suite de quotients incomplets, forme une suite indéfinie dans laquelle un certain nombre de termes se reproduit indéfiniment et dans le même ordre [1].

Soit $x = \frac{\sqrt{A} + N}{D}$ la quantité donnée que nous supposons être positive et soit

$$x_k = \frac{\sqrt{A} + N_k}{D_k},$$

le quotient complet d'ordre k.

On a
$$N_n^2 + D_n D_{n-1} = A,$$
$$N_{n+1} + N_n = a_{n+1} D_n .$$

De plus, les nombres N_n et D_n sont des nombres entiers et, à partir d'un certain rang, positifs. Considérons le développement à partir de ce rang, alors

$$N_n < \sqrt{A},$$
$$D_n < 2\sqrt{A}.$$

Ainsi les quantités N_n et D_n sont limitées supérieurement.

Il en résulte que les quotients complets x_k ($k = 1, 2, 3, \ldots$) ne peuvent avoir qu'un nombre limité de valeurs différentes.

Donc après un certain nombre d'opérations, plus ou moins long on retombera nécessairement sur un quotient complet déja obtenu.

Si $x_{k+i} = x_k$ on aura $x_{k+i+m} = x_{k+m}$ ($m = 1, 2, 3, \ldots$) et la suite des quotients complets

$$x_k, \quad x_{k+1}, \quad x_{k+2}, \quad \ldots,$$

---

[1] Lagrange. Œuvres II, p. 74. La réciproque fut connue d'Euler.

ainsi que la suite que les quotients incomplets

$$a_{k+1}, \quad a_{k+2}, \quad a_{k+3}, \quad \ldots,$$

se reproduira indéfiniment dans le même ordre.

11. Réciproquement, toute fraction continue périodique est une racine d'une équation de second degré.

Considérons d'abord une fraction continue simple, c'est-à-dire, dans laquelle la période commence à partir du premier terme.

Soit $$x = a_1, a_2, a_3, \ldots, a_n, a_1, a_2, a_3, \ldots,$$

cette fraction, que nous écrirons en abrégé

$$x = (a_1, a_2, a_3, \ldots, a_n).$$

Puisque $x_{n+1} = x_1 = x_{kn+1}$, on aura

$$x = a_1, a_2, a_3, \ldots, a_n, x,$$

ou si on désigne par $\frac{p_n}{q_n}$ la $n^{ième}$ réduite

$$x = \frac{p_n x + p_{n-1}}{q_n x + q_{n-1}}, \quad \text{ou} \quad q_n x^2 + (q_{n-1} - p_n) x - p_{n-1} = 0, \quad (7)$$

ce qui démontre le théorème.

Si ensuite x est une fraction continue périodique mixte, posons

$$x = a_1, a_2, \ldots, a_k, a_{k+1}, a_{k+2}, \ldots, a_{k+n}, a_{k+1}, \ldots,$$

que nous écrirons en abrégé

$$x = a_1, a_2, a_3, \ldots, a_k (a_{k+1}, \ldots, a_{k+n}).$$

On aura alors

$$x = \frac{p_k x_{k+1} + p_{k-1}}{q_k x_{k+1} + q_{k-1}} = \frac{p_{k+n} x_{k+n+1} + p_{k+n-1}}{q_{k+n} x_{k+n+1} + q_{k+n-1}},$$

et puisque $x_{k+1} = x_{k+n+1}$, il vient

$$x_{k+1} = x_{k+n+1} = \frac{q_{k-1} x - p_{k-1}}{q_k x - p_k} = \frac{q_{k+n-1} x - p_{k+n-1}}{q_{k+n} x - p_{k+n}}, \quad (8)$$

qui est une équation du second degré.

Remarques.— 1° Si x_1 et x_2 sont les deux racines de (7) on aura

$$-1 < x_1 < 0 < 1 < x_2,$$

En effet $f(x)$ désignant le premier membre de (7) on trouve

$$f(-1) = q_n - q_{n-1} + p_n - p_{n-1} > 0,$$

$$f(0) = -p_{n-1} < 0,$$

$$f(1) = (q_n - p_n) + (q_{n-1} - p_{n-1}) < 0 \quad \text{puisque } \frac{p_k}{q_k} > 1,$$

$$f(\infty) = +\infty > 0,$$

ce qui permet de séparer les deux racines de (7).

Réciproquement, si une quantité x se développe en fraction continue périodique simple, elle est positive et plus grande que 1. Elle est racine d'une équation du second degré dont la racine conjuguée est comprise entre (-1) et 0.

2° La condition nécessaire et suffisante pour qu'un nombre algébrique du second degré x donne naissance à une fraction continue périodique simple est

$$x > 1,$$

$$-1 < x' < 1,$$

x' étant le nombre algébrique conjugué de x.

3° Si $k = 1$, c'est-à-dire s'il n'y qu'un seul terme non périodique, on aura

a) $\qquad x_1 > 0 \quad$ et $\quad x_2 > 0,$

ou bien

b) $\qquad x_1 x_2 < 0 \quad$ et si $\quad x_1 < 0, \quad x_2 > 0,$

on aura $\qquad x_1 < -1.$

4° Si $k = 2$, c'est-à-dire s'il y a deux termes dans la partie non périodique, soit

$$x = a, b\,(a_1, a_2, \ldots, a_k),$$

le développement de x, on aura

a) $a \neq 0$, les deux racines de l'équation (8) sont toutes les deux positives.

$$b)\ a = 0 \begin{cases} \text{Si } b > a_k, \text{ les deux racines de (8) sont positives.} \\ \text{Si } b < a_k, \text{ les racines sont des signes contraires et} \\ \quad \text{la racine positive est } < 1. \end{cases}$$

5° Si $k > 2$, toutes les deux racines sont positives.

12. Théorème. — Les périodes des quotients incomplets dans les fractions continues qui expriment les deux racines d'une équation du deuxième degré à coefficients entiers, sont inverses l'une à l'autre, c'est-à-dire que les quotients dont se compose l'une des périodes sont ceux de l'autre période disposée dans un ordre inverse.

Supposons d'abord que la racine considerée donne naissance à une fraction périodique simple. On peut supposer que cette racine est > 1, sinon, on change x en $-\frac{1}{x}$.

On a

$$x = \frac{p_n x_{n+1} + p_{n-1}}{q_n x_{n+1} + q_{n-1}}, \qquad \text{d'où} \qquad x_{n+1} = \frac{q_{n-1} x - p_{n-1}}{p_n - q_n x},$$

et l'équation est donc

$$x = \frac{q_{n-1} x - p_{n-1}}{p_n - q_n x}.$$

Soit $-\frac{1}{y}$ la seconde racine, il vient

$$y = \frac{p_n y + q_n}{p_{n-1} y + q_{n-1}}.$$

Or $\frac{p_n}{q_n}$ est par hypothèse > 1 donc les développements de $\frac{p_n}{q_n}$ et $\frac{p_n}{q_{n-1}}$ sont inverses l'un à l'autre.

De plus $\frac{q_n}{q_{n-1}}$ est l'avant-dernière réduite dans la suite de réduite de $\frac{p_n}{p_{n-1}}$, donc y se développe en une fraction continue périodique simple, dont la période est inverse à celle de la fraction x.

Soit ensuite une racine d'une équation donnant naissance à une fraction périodique mixte. Supposons que cette racine soit positive. Soit

$$x = a_1, a_2, \ldots, a_m\,(a_{m+1}, \ldots, a_{m+k}),$$

d'où
$$x = \frac{p_m\, x_{m+1} + p_{m-1}}{q_m\, x_{m+1} + q_{m-1}}, \tag{9}$$

x_{m+1} étant supérieur à 1, x_m se développe en une fraction continue périodique simple, et la seconde racine étant $-\frac{1}{y}$, y et x_m ont des périodes qui sont inverses l'une à l'autre.

Donc (1) donne la seconde racine si on y remplace x_m par y

$$y = \frac{p_{m-1}\, y_{m+1} - p_m}{q_{m-1}\, y_{m-1} - q_m}.$$

Puisqu'on a
$$p_n\, q_{n-1} - q_n\, p_{n-1} = (-1)^n,$$

y et y_{m+1} se terminent par le même quotient (T. II, I. 8).

D'ailleurs dans une fraction continue périodique, on est libre de fixer le commencement de la période ou on veut, après la partie qui est réellement non périodique.

Corollaire. — Les périodes des quotients complets dans les fractions continues qui expriment les deux racines d'une équation de second degré sont inverses l'une à l'autre, c'est-à-dire que les quotients complets dont se compose l'une des périodes, sont ceux de l'autre période disposée dans un ordre inverse.

13. Considérons un cas particulier très important, celui du développement de la racine positive de l'équation $x^2 - A = 0$, A n'étant pas un carré parfait, mais un entier positif.

Le développement de $\sqrt{A}$ sera périodique mixte, car x' (conjugué de x) n'est pas compris entre -1 et 0, $x' = -\sqrt{A} < -1$,

Soit a l'entier contenu dans $\sqrt{A}$, si on fait $y = x + a$, le conjugué x' devient $y' = -\sqrt{A} + a$ et on aura $-1 < y' < 0$ et $y > 1$. Il en résulte que le développement de $y = \sqrt{A} + a$ est une fraction continue périodique simple.

Soit
$$y = (x_0, x_1, x_2, \ldots, x_k).$$

On aura d'abord $x_0 = 2a$, car a étant le plus grand entier contenu dans $\sqrt{A}$, celui de y est $2a$, ainsi

$$y = (2a, x_1, x_2, \ldots, x_k),$$

ou encore $$y = 2a\,(x_1, x_2, \ldots, x_k, 2a),$$

ce qui donne

$$x = y - a = a\,(x_1, x_2, \ldots, x_k, 2a).$$

La suite $x_1, x_2, \ldots, x_k$ est symétrique, car le développement de $\sqrt{A} + a$ est

$$\sqrt{A} + a = (2a, x_1, x_2, x_3, \ldots, x_k),$$

et celui de la racine conjuguée donne

$$\sqrt{A} + a = (2a, x_k, x_{k-1}, \ldots, x_1),$$

il en résulte qu'on aura

$$x_1 = x_k, \qquad x_2 = x_{k-1}, \qquad \ldots, \qquad x_i = x_{k-i+1}.$$

Ainsi le développement de $\sqrt{A}$ sera

$$\sqrt{A} = a\,(x_1, x_2, x_3, \ldots, x_k, 2a),$$

la suite $x_1, x_2, \ldots, x_k$ étant symétrique et a l'entier contenu dans $\sqrt{A}$.

14. Le Chapitre III sera entièrement consacré à l'étude de la période des quotients incomplets de $\sqrt{A}$. Pour le moment, nous nous bornerons à l'étude de la période des quotients complets.

Soit $$x_i = \frac{\sqrt{A} + N_i}{D_i} = a_{i+1} + \frac{1}{x_{i+1}}$$

et considérons la suite des quotients complets x_i

$$\frac{\sqrt{A} + a}{D_1}, \quad \frac{\sqrt{A} + N_2}{D_2}, \quad \frac{\sqrt{A} + N_3}{D_3}, \quad \ldots,$$

$$\frac{\sqrt{A} + N_{k-1}}{D_2}, \quad \frac{\sqrt{A} + N_k}{D_2}, \quad \frac{\sqrt{A} + a}{1}.$$

A cette suite des quotients complets correspond la suite

$$a, \quad x_1, \quad x_2, \quad x_3, \quad \ldots, \quad x_{k-1}, \quad x_k, \quad 2a,$$

des quotients incomplets et la suite

$$\frac{a}{1}, \quad \frac{p_1}{q_1}, \quad \frac{p_2}{q_2}, \quad \ldots, \quad \frac{p_{k-1}}{q_{k-1}}, \quad \frac{p_k}{q_k}, \quad \frac{p_{k+1}}{q_{k+1}},$$

des réduites successives.

Nous nous bornerons à signaler les théorèmes suivants

1° $p_i^2 - Aq_i^2 = \pm D_{i+1}$.

2° $N_i + N_{k-i} = D_i\, a_{i+1}$.

3° Si k est impair, soit $k = 2i + 1$, alors

$$N_{i+1} \quad \text{divise} \quad a_{i+1}.D_{i+1}.$$

4° Si k est pair, soit $k = 2i$, alors

$$x_i = \frac{\sqrt{A} + N_i}{D_i} \quad \text{et} \quad x_{i+1} = \frac{\sqrt{A} + N_{i+1}}{D_{i+1}}.$$

On aura $\quad D_i = D_{i+1}, \quad N_i + N_{i+1} = a_{i+1}.D_i$

et enfin $\quad A = D_i^2 + Z^2$.

15. Soit $\sqrt{A} = a\,(a_1, a_2, \ldots, a_k, 2a)$ le développement de $\sqrt{A}$ en fraction continue et soit $x_i = \dfrac{\sqrt{A} + N_i}{D_i} = a_{i+1} + \dfrac{1}{x_{i+1}}$ les quotients complets et incomplets d'un certain rang.

Soit $\dfrac{p_i}{q_i}$ la réduite d'ordre i

$$\frac{p_i}{q_i} = a, a_1, a_2, \ldots, a_i\ .$$

On aura

$$\sqrt{A} = \frac{p_i\, x_{i+1} + p_{i-1}}{q_i\, x_{i+1} + q_{i-1}} = \frac{p_i\, \dfrac{\sqrt{A} + N_{i+1}}{D_{i+1}} + p_{i-1}}{q_i\, \dfrac{\sqrt{A} + N_{i+1}}{D_{i+1}} + q_{i-1}}.$$

Ce qui donne

$$q_i\, N_{i+1} + q_{i-1}\, D_{i+1} = p_i\ ,$$

$$p_i\, N_{i+1} + p_{i-1}\, D_{i+1} = Aq_i\ .$$

En résolvant ces équations par rapport à N_{i+1} et D_{i+1}, on trouve

$$\frac{N_{i+1}}{Aq_i\, q_{i-1} - p_i p_{i-1}} = \frac{D_{i+1}}{p_i^2 - Aq_i^2} = \frac{1}{p_i\, q_{i+1} - q_i\, p_{i-1}} = \pm 1,$$

d'où $\quad \pm D_{i+1} = p_i^2 - Aq_i^2\ .$

On sait (T. II. I. 5) que si l'équation $x^2 - Ay^2 = \pm D$ est possible ($D < \sqrt{A}$) la fraction $\dfrac{x}{y}$ est une des réduite de $\sqrt{A}$.

Il résulte de ce qui précède que cette équation est effectivement possible, si parmi les quotients complets, on en trouve un dont le dénominateur est D. Dans le cas contraire l'équation $x^2 - Ay^2 = D$ ($D < \sqrt{A}$) est impossible.

Cette équation est toujours possible si $D = +1$, car

$$x_{k+1} = \frac{\sqrt{A} + a}{1} = 2a + \frac{1}{x_{k+2}} \text{ donne } D_{k+1} = 1.$$

16. Un deuxième cas particulier d'une équation de second degré est celui de l'équation

$$x^2 + x - A = 0 \text{ (A étant un entier positif).}$$

Le développement de x en fraction continue sera :

1° *Périodique mixte.*

2° *Il y aura un seul terme précédant la période; soit* a *le terme.*

3° *Le dernier terme de la période est* $2a + 1$.

4° *Abstraction faite de ce terme, la période est symétrique.*

1° Soit x' la racine conjuguée de x. Comme x' n'est pas compris entre -1 et 0, x ne peut pas être une fraction périodique simple.

Si on fait

$$y = x + a + 1,$$

on aura

$$-1 < y' < 0,$$

et

$$y = (2a + 1, x_1, x_2, x_3, \ldots, x_k),$$

ou

2° $$y = 2a + 1\ (x_1, x_2, x_3, \ldots, x_k, 2a + 1),$$

ce qui donne

3° $$x = a\ (x_1, x_2, x_3, \ldots, x_k, 2a + 1).$$

4° On trouve par le développement de y

$$y = (2a + 1, x_1, x_2, x_3, \ldots, x_k)$$

et d'autre part ce développement peut être obtenu comme celui de la racine conjuguée

$$y = (2a + 1, x_k, x_{k-1}, \ldots, x_1),$$

ce qui donne

$$x_i = x_k,\ x_2 = x_{k-1},\ \ldots,\ x_i = x_{k-1}.$$

Le Chapitre IV sera consacré à l'étude du développement de la période des quotients incomplets. Pour le moment, remarquons que les notations étant celles que nous avons employées dans le numéro 14, toutes les formules subsistent, la première seule devant subir une légère modification et s'écrire $p_i^2 + p_i q_i - Aq_i^2 = \pm D_{i+1}$.

CHAPITRE II.

Équation indéterminée du second degré à deux inconnues.

1. Nous désignons par f le polynome du second degré à deux variables

$$f = Ay^2 + 2Bxy + Cx^2 + 2Dy + 2Ex + F, \qquad (1)$$

et nous allons étudier l'équation indéterminée $f = 0$.

Les coefficients du polynome représenté par f sont quelconques, mais rationnels. On peut dès lors les supposer entiers, tant qu'il s'agit de l'équation $f = 0$.

En géométrie analytique l'équation $f = 0$ représente une conique (proprement dite ou dégénérée, réelle ou imaginaire). Il en est ainsi si x et y varient d'une façon continue. Mais il ne peut être question d'une courbe représentative, quand on se borne aux valeurs entières de x et y.

Toutefois, nous emprunterons le langage géométrique qui nous sera utile par la précision des termes employés en géométrie.

Ainsi, résoudre en nombres entiers l'équation $f = 0$ revient à trouver des points entiers (points dont les deux coordonnées sont entières) sur la conique $f = 0$.

Rappelons que si $f = 0$ représente une ellipse ou une hyperbole on trouve *le centre* $(x_0 y_0)$ de la conique $f = 0$ en résolvant les deux équations

$$Ay_0 + Bx_0 + D = 0, \qquad By_0 + Cx_0 + E = 0.$$

ce qui donne

$$\frac{x_0}{DB - AE} = \frac{y_0}{BE - CD} = \frac{1}{AC - B^2},$$

et dans ce cas f peut être mis sous la forme

$$f = A(y - y_0)^2 + 2B(y - y_0)(x - x_0) + C(x - x_0)^2 - H, \qquad (2)$$

étant posé $H = -(Dy_0 + Ex_0 + F)$.

Si on fait *une translation des axes* de manière à ce que l'origine vienne au centre (par les formules $x = X + x_0$, $y = Y + y_0$), on trouve

$$f = AY^2 + 2BXY + CX^2 - H. \tag{3}$$

2. Considérons d'abord le cas de l'ellipse.

Soit $f = 0$ l'équation d'une ellipse et cherchons *toutes les solutions entières* de cette équation. Le centre de l'ellipse étant rationnel, soit (x_0, y_0) ce centre.

Posons $\qquad x = X + x_0, \qquad y = Y + y_0 \qquad$ (1) devient

$$AY^2 + 2BXY + CX^2 = H, \tag{3}$$

multiplions (3) par A, on trouve

$$(AY + BX)^2 + (AC - B^2)\,X^2 = AH,$$

ou enfin

$$t^2 + \Delta u^2 = AH, \tag{4}$$

en posant

$$AY + BX = t \qquad AC - B^2 = \Delta, \qquad X = u.$$

L'équation (4) représente la même ellipse que (1), mais la courbe est rapportée à ses axes dans (4), tandis que les axes sont quelconques dans (1). En d'autres termes les axes de la courbe sont les axes coordonnés dans (4). Les axes coordonnés sont quelconques dans (1).

Si $AH < 0$, (4) est une ellipse imaginaire, ainsi que (1) et il n'y a pas dans ce cas de solutions entières.

Si $H = 0$, (4) est une ellipse évanouissante, admettant le seul point entier $t = u = 0$. Si à ces valeurs de t et u correspondent des valeurs entières de x, y, on aura une solution entière de (1). Dans le cas contraire (1) est impossible.

Dans le cas général $AH > 0$. On cherchera alors *toutes les solutions entières* de (4). Chaque solution de (4) conduit à un point rationnel (xy) de (1). Si ce point est entier, on aura une solution de (1).

Nous remarquerons que *si il y a des points entiers sur une ellipse, ils sont en nombre fini.*

Il est évident que tous ce que nous avons dit de l'ellipse s'applique aussi au cercle $\left(\frac{A}{1} = \frac{B}{\cos\theta} = \frac{C}{1}\right.$ et, en axes rectangulaires, comme c'est généralement le cas, $A = C$, $B = 0$),

Exemple

$$f = y^2 + 4xy + 7x^2 - 16y - 50x = 0.$$

Le centre (xy) de cette ellipse est donné par les équations

$$2y + 4x - 16 = 0, \qquad 4y + 14x - 50 = 0,$$

d'où

$$\frac{y}{2} = \frac{x}{3} = 1.$$

On peut alors mettre f sous la forme

$$(y-2)^2 + 4(y-2)(x-3) + 7(x-3)^2 = 91,$$

ou bien

$$Y^2 + 4XY + 7X^2 = 91,$$

ou enfin

$$(Y + 2X)^2 + 3X^2 = 91,$$

d'où

$$\begin{aligned} &Y + 2X = \pm 8, \quad \pm 4, \\ &X = \pm 3, \quad \pm 5, \\ &Y = \pm 2, \ \pm 14, \quad \pm 6, \quad \pm 14. \end{aligned}$$

On a ainsi les solutions suivantes

$X =$	$+3$	$+3$	-3	-3	$+5$	$+5$	-5	-5
$Y =$	2	-14	-2	$+14$	-6	-14	$+6$	$+14$

on remonte aux inconnues primitives x, y par les formules

$$x = X + 3, \qquad y = Y + 2,$$

ce qui donne

$x = 6$	6	0	0	8	8	-2	$-2,$
$y = 4$	-12	0	16	-4	-12	8	$16.$

3. Considérons en deuxième lieu le cas d'une parabole. Alors un des coefficients A ou C n'est pas nul, car $B^2 - AC = 0$ et si $A = C = 0$, on aurait $B = 0$ et (1) serait du premier degré ; soit donc $A \neq 0$, il vient

$$Af = (Ay + Bx + D)^2 + 2(AE - BD)x + (AF - D^2) = 0. \quad (5)$$

Dans le cas particulier quand AE = BD la parabole (1) est constituée par deux droites parallèles

$$(Ay + Bx + D)^2 = (D^2 - AF),$$

réelles, confondues ou imaginaires. L'équation (1) est aussi remplacée par deux équations linéaires (réelles, identiques ou imaginaires). Dans le premier cas, il faut encore que $D^2 - AF$ soit un carré parfait pour avoir des solutions entières.

Si AE — BD n'est pas nul (5) s'écrit

$$t^2 + u = 0, \tag{6}$$

en posant

$$\left.\begin{aligned} Ay + Bx + D &= t, \\ 2\,(AE - BD)\,x + (AF - D^2) &= u. \end{aligned}\right\} \tag{7}$$

Les solutions de (5) sont données par les formules générales

$$\left.\begin{aligned} u &= -e^2, \\ t &= e, \end{aligned}\right\} \tag{8}$$

qui déterminent les valeurs suivantes de x et y

$$\left.\begin{aligned} x &= \frac{+e^2 + (AF - D^2)}{2\,(BD - AE)}, \\ y &= \frac{2\,(BD - AE)\,e - Be^2 - B(AF - D^2)}{2A\,(BD - AE)}. \end{aligned}\right\} \tag{9}$$

Si ces valeurs peuvent être rendues entières, on aura des solutions entières de (1). Dans le cas contraire (1) est impossible.

Exemples : 1° Soit l'équation

$$9y^2 - 12xy + 4x^2 - 30y + 23 + 2 = 0,$$

ou

$$(3y - 2x - 5)^2 + (3x - 4) = 0.$$

On aura

$$(3y - 2x - 5 = t,$$

$$3x - 4 = -t^2,$$

d'où

$$x = \frac{-t^2 + 4}{3}, \qquad y = \frac{3t - 2t^2 + 23}{9}.$$

Pour que x soit entier il faut qu'on ait $t \equiv \pm 1$ (Mod. 3).

" y " " $t \equiv 7$ ou 8 (Mod. 9).

Posons $t = 9e + 7$, il vient

$$x = -(27e^2 + 42e + 15),$$

$$y = -(18e^2 + 25e + 6).$$

Si $t = 9e + 8$, on trouve

$$x = -(27e^2 + 48e + 20),$$

$$y = -(18e^2 + 29e + 9).$$

2° Soit l'équation

$$25y^2 + 30xy + 9x^2 - 60y - 43x + 41 = 0,$$

ou

$$(5y + 3x - 6)^2 - (7x - 5) = 0.$$

On peut donc poser

$$5y + 3x - 6 = t, \qquad 7x - 5 = t^2,$$

d'où

$$x = \frac{t^2 + 5}{7}, \qquad y = \frac{7t - 3t^2 + 27}{35}.$$

La première de ces équations donne $t = \pm 3$ (Mod. 7).

Mais la deuxième donne $t^2 + t + 1 \equiv 0$ (Mod. 5) congruence impossible [1].

L'équation donnée n'a pas de solutions entières.

Remarques.— 1° Dans le premier exemple, on trouve deux solutions qui paraissent indépendantes

$$-x = 27e^2 + 42e + 15, \qquad 27e^2 + 48e + 20,$$

$$-y = 18e^2 + 25e + 6, \qquad 18e^2 + 29e + 9.$$

Or chacune de ces solutions donne *tous* les points entiers de la courbe quand on donne à e toutes les valeurs possibles.

Il en résulte que ces deux solutions se déduisent l'une de l'autre par une substitution linéaire.

Ainsi, si dans

$$x = -(27e^2 + 42e + 15),$$

$$y = -(18e^2 + 25e + 6),$$

---

[1] On peut écrire $(2t + 1)^2 + 3 \equiv 0$ ou $(2t + 1)^2 \equiv 2$ (Mod. 5) ce qui est impossible puisque $\left(\frac{2}{5}\right) = -1$.

on fait $e = f + \frac{1}{9}$, il vient

$$x = -(27f^2 + 48f + 20), \qquad y = -(18f^2 + 29f + 9),$$

ce qui est la deuxième solution. Inversement on transforme la deuxième solution en la première en faisant

$$e = f - \frac{1}{9}.$$

2° Observons encore que si il y a des points entiers sur une parabole (proprement dite ou dégénérée), ils sont en nombre illimité.

4. Le cas le plus important est celui quand (1) est du genre hyperbole. Par une translation au centre on ramènera (1) à la forme

$$AY^2 + 2BXY + CX^2 = H. \tag{3}$$

Avant d'étudier le cas général, remarquons qu'on peut résoudre (3) facilement dans les cas suivants :

1° Un des coefficients A ou C est nul. Le premier membre de (3) se décompose de deux facteurs linéaires, la deuxième en deux facteurs numériques (de toutes les manières possibles) λ et $\frac{H}{\lambda}$ qu'on égalera aux deux facteurs linéaires.

Si $A = 0$, on aura

$$X(2BY + CX) = H = \lambda \cdot \frac{H}{\lambda},$$

d'où

$$X = \lambda, \qquad 2BY + CX = \frac{H}{\lambda}.$$

2° Si $B^2 - AC$ est un carré parfait, posons $B^2 - AC = d^2$ (3) devient

$$(AY + BX)^2 + (AC - B^2)X^2 = AH,$$

ou

$$(AY + BX)^2 - d^2X^2 = AH,$$

ou

$$\left\{AY + (B + d)X\right\}\left\{AY + (B - d)X\right\} = AH = \lambda \cdot \frac{AH}{\lambda},$$

on décomposera cette équation en deux

$$\left.\begin{aligned} AY + (B + d)X &= \lambda, \\ AY + (B - d)X &= \frac{AH}{\lambda}. \end{aligned}\right\} \tag{10}$$

On donnera à λ toutes les valeurs divisant AH et telles que X et Y qui résultent de (10) soient entières.

On remarquera, en outre, que dans (3) A, 2B et C sont premiers entre eux, car leur commun diviseur, s'il existait, diviserait aussi H et ce facteur pourrait être écarté de deux membres de (3).

Enfin les valeurs des inconnues X et Y doivent aussi être premières entre elles, car si X et Y admettent un diviseur commun d, H est divisible par d^2 et ce facteur pourrait être écarté.

5. Dans le cas général l'équation

$$AY^2 + 2BXY + CX^2 = H, \tag{3}$$

est telle que ni A ni C ne sont nuls, et $B^2 - AC$ n'est pas un carré parfait.

Si (3) a des solutions, le rapport $\frac{Y}{X}$ est rationnel et on peut poser $\frac{Y}{X} = z$, (3) donne alors

$$Az^2 + 2Bz + C \equiv 0 \text{ (Mod. H)}. \tag{11}$$

Si la congruence caractéristique (11) n'est pas possible, l'équation (3) ne l'est pas non plus. Dans le cas contraire posons

$$Y = zX + HT, \tag{12}$$

(3) devient

$$\frac{Az^2 + 2Bz + C}{H} X^2 + 2(Az + B)XT + AHT^2 = 1. \tag{13}$$

Dans (13) le coefficient de X^2 est entier en vertu de (11).

L'équation (13) est donc de la même forme que (3), mais le deuxième membre est 1.

Le déterminant de l'équation (13) est

$$(Az + B)^2 - A(Az^2 + 2Bz + C) = B^2 - AC \text{ — celui de (3)}$$

ce qui confirme que la quantité $B^2 - AC$ est un invariant de (3).

Remarque. Pour transformer (3) en (13) il faut résoudre la congruence du second degré

$$Az^2 + 2Bz + C \equiv 0 \text{ (Mod. H)}. \tag{11}$$

Elle est possible si $\left(\frac{B^2 - AC}{H}\right) = +1$, car (11) donne

$$(Az + B)^2 \equiv B^2 - AC \text{ (Mod. H)}.$$

congruence qui exige que $(B^2 - AC)$ soit résidu quadratique de H.

Si l'équation (3) est possible, elle donne

$$(AY + BX)^2 = (B^2 - AC)\,X^2 - AH, \quad \text{ou} \quad \text{(Mod. H)},$$

$$(AY + BX)^2 \equiv (B^2 - AC)\,X^2,$$

congruence qui prouve que $(B^2 - AC)$ est résidu de H.

La réciproque est vraie pour (11) mais non pour (3).

En d'autres termes, si $(B^2 - AC)$ est résidu de H, la congruence (11) est possible, mais l'équation (3) peut ne pas l'être.

6. Par ce qui précède, l'équation générale du second degré à deux inconnues est ramenée, dans le cas où elle est du genre hyperbole, à la forme spéciale (13) où le deuxième membre est 1 et le premier une *forme binaire trinome quadratique* [1].

La transformation suivante que nous avons à effectuer a pour but de *réduire* cette forme. La réduction dépend essentiellement de la nature du coefficient de xy. Aussi, devons nous considérer les deux cas qui peuvent se présenter.

Nous ferons ultérieurement une étude spéciale des formes quadratiques et de leur réduction. Dans ce qui suit nous nous occupons exclusivement de la réduction de (13).

7. Soit d'abord le cas ou le coefficient de xy est pair. Nous écrirons l'équation (13) sous la forme

$$ay^2 + 2bxy + cx^2 = 1, \tag{14}$$

le changement de notation étant destiné à bien marquer que le point de départ des calculs ultérieurs est (14).

Les trois coefficients de cette équation sont entiers, celui du milieu étant en plus pair.

---

[1] La forme (13) est binaire par ce qu'elle contient deux variables. Elle est trinome parce que le premier membre contient trois termes.

Supposons qu'on ait une solution particulière de (14),

$$x = x_0, \qquad y = y_0, \tag{15}$$

et considérons la substitution

$$\left.\begin{aligned} y &= y_0 t - (by_0 + cx_0)\, u, \\ x &= x_0 t + (ay_0 + bx_0)\, u. \end{aligned}\right\} \tag{16}$$

Cette substitution est *modulaire* [1] car

$$y_0 (ay_0 + bx_0) + x_0 (by_0 + cx_0) = ay_0^2 + 2bx_0 y_0 + cx_0^2 = +1,$$

de sorte qu'aux valeurs entières de x et y correspondent des valeurs entières de u et t et inversement.

Si on effectue la substitution (16), l'équation (14) devient

$$(ay_0^2 + 2bx_0 y_0 + cx_0^2)\, t^2 - (b^2 - ac)(ay_0^2 + 2bx_0 y_0 + cx_0^2)\, u^2 = 1,$$

ou en vertu de (14) dont (15) est une solution

$$t^2 - \mathrm{A} u^2 = 1, \tag{17}$$

étant posé $\qquad \mathrm{A} = b^2 - ac.$

Ainsi, si on connaît une solution particulière de (14), on transforme (14) par (16) et on obtient (17).

8. Considérons en deuxième lieu l'équation (13) dans le cas ou le rectangle des variables a un coefficient impair.

Soit

$$ay^2 + (2b + 1)\, xy + cx^2 = 1. \tag{14^{bis}}$$

l'équation (13) donnée, le changement de notation étant destiné à bien remarquer que le point de départ des calculs ultérieurs est l'équation (14bis). Les trois coefficients de cette équation sont entiers, celui du milieu est impair.

---

[1] Une substitution $\left\{\begin{aligned} x &= \alpha x' + \beta y' \\ y &= \gamma x' + \delta y' \end{aligned}\right\}$ est modulaire, quand son déterminant $\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix}$ est égal à $+1$.

Dans ce cas aux valeurs entières de x', y' correspondent des valeurs entières de x, y et réciproquement.

Supposons qu'on ait une solution particulière

$$y = y_0, \qquad x = x_0, \tag{15^{bis}}$$

et considérons la substitution

$$\left.\begin{aligned} y &= y_0 t - (by_0 + cx_0)\, u, \\ x &= x_0 t + [ay_0 + (b+1)\, x_0]\, u. \end{aligned}\right\} \tag{16^{bis}}$$

Elle est modulaire, car

$$y_0(ay_0 + bx_0 + x_0) + x_0(by_0 + cx_0) = ay_0^2 + (2b+1)\,xy + cx_0^2 = +1,$$

de sorte qu'aux valeurs entières de x et y correspondent des valeurs entières de u et t et inversement.

Si on effectue la substitution (16bis), l'équation (14bis) devient

$$\{ ay_0^2 + (2b+1)\, x_0 y_0 + cx_0^2 \}\, t^2 + \{ ay_0^2 + (2b+1)\, x_0 y_0 + cx_0^2 \}\, tu$$
$$+ (ac - b^2 - b) \{ ay_0^2 + (2b+1)\, x_0 y_0 + cx_0^2 \}\, u^2 = +1,$$

ou bien en vertu de (14bis) dont (15bis) est une solution

$$t^2 + tu + (ac - b^2 - b)\, u^2 = 1,$$

ou enfin

$$t^2 + tu - \mathrm{A}u^2 = 1, \tag{17^{bis}}$$

étant posé

$$\mathrm{A} = b^2 + b - ac.$$

On remarquera que le déterminant de (14bis) et (17bis) est le même car

$$(2b+1)^2 - 4ac = 1 - 4\,(ac - b^2 - b).$$

Ainsi si on connaît une solution particulière de (14bis) on transforme (14bis) par (16bis) et on obtient (17bis).

9. Ainsi qu'on l'a vu aux numéros 7 et 8, on ramène l'équation (13) à l'équation

$$t^2 - \mathrm{A}u^2 = +1, \tag{17}$$

ou

$$t^2 + tu - \mathrm{A}u^2 = +1, \tag{17^{bis}}$$

selon que dans (13) le coefficient du deuxième terme est pair ou impair.

Ce sont les formes réduites de (13).

Puisque (17) est plus simple que (17bis), nous signalerons un cas quand (17bis) se transforme en (17).

C'est le cas ou A est pair.

Alors u est pair et t impair. Posons dans (17bis)

$$t = y - x, \qquad u = 2x,$$

on trouve

$$y^2 - (4A + 1)\, x^2 = +1,$$

ce qui est bien l'équation (17).

La transformation que nous avons faite de (17bis) en (17) est applicable, quel que soit A, mais si A est impair, elle donne seulement les solutions de (17bis) dans lesquelles u est pair.

La résolution effective des équations (17) et (17bis) dépend du développement en fraction continue de la racine de l'équation

$$x^2 - A = 0,$$

$$x^2 + x - A = 0.$$

C'est de ce développement que nous allons nous occuper dans les deux chapitres suivants.

Le développement de la racine de l'équation $x^2 - A = 0$ étant de loin le plus important, nous l'examinerons avec plus de détails.

CHAPITRE III.

Développement en fraction continue de la racine positive de l'équation $x^2 = A$.

1. Considérons un nombre entier $A = a^2 + b$ $(b \leqslant 2a)$ non carré parfait et le développement de $\sqrt{A}$ en fraction continue.

On aura

$$\sqrt{A} = a, x_1, x_2, x_3, \ldots, \qquad x_{k-1}, x_k, \ldots.$$

Ce développement est illimité et indéfiniment périodique. La période commence par le deuxième quotient incomplet et comprend $k + 1$ termes, dont le dernier est $2a$, les k autres termes formant une suite symétrique.

On aura ainsi

$$\sqrt{A} = a\,(x_1, x_2, x_3, \ldots, x_{k-1}, x_k, 2a), \qquad \text{(I)}$$

avec les relations $\qquad x_i = x_{k-i+1}.$ $\qquad$ (T. II. p. 15)

2. Inversement, si le développement d'une quantité x est (1) cette quantité x est racine de l'équation $x^2 = A$.

Soit $\qquad x = a\,(x_1, x_2, \ldots, x_k, 2a),$

ou $\qquad x - a = 0, x_1, x_2, x_3, \ldots, x_k, x + a.$

Posons $\qquad \dfrac{P}{Q} = 0, x_1, x_2, x_3, \ldots, x_k,$

et soit $\dfrac{R}{P}$ [1] la réduite qui précède $\dfrac{P}{Q}$ dans le développement de $x - a$.

---

[1] A cause de la symétrie de la suite des quotients incomplets

$$x_1, x_2, \ldots, x_k,$$

le numérateur de la réduite $0, x_1, x_2, x_3, x_4, \ldots, x_k$ est égal au dénominateur de la réduite $0, x_1, x_2, x_3, \ldots, x_{k-1}$ (T. II. p. 7).

On aura $$x - a = \frac{P(x+a) + R}{Q(x+a) + P},$$

ou $$Q(x^2 - a^2) = 2aP + R,$$

ou enfin $$x^2 = a^2 + \frac{2aP + R}{Q}.$$

Cette expression montre que tout développement de la forme (1) provient de $\sqrt{A}$, mais A ne sera pas toujours entier. Pour que A soit entier il faut que $2aP + R$ soit divisible par Q.

3. On peut avoir $k = 0$. La période est alors constituée uniquement par le seul terme irrégulier et on aura

$$\sqrt{A} = a\,(2a), \qquad \text{ou} \qquad \sqrt{A} - a = \frac{1}{\sqrt{A} + a},$$

d'où $$A = a^2 = 1,$$

et $$\sqrt{a^2 + 1} = a\,(2a), \tag{1}$$

formule qui ne contient qu'un seul paramètre a. On trouve pour $a = 1$ le développement connu d'Euclide. On aura ainsi le développement des nombres $\sqrt{A}$, avec A =

2	5	10	17	26	37	50	65	82	101	122	145
170	197	226	257	290	325	362	401	442	485	530	577
626	677	730	785	842	901	962,	etc.,				

en faisant dans (1) $a = 1, 2, 3, \ldots$, etc.

4. Il peut arriver que la période soit constituée d'un seul terme dans la partie symétrique.

Soit $$\sqrt{A} = a\,(x, 2a),$$

un tel développement. On trouve

$$\sqrt{A} - a = 0, \quad x, \quad \sqrt{A} + a,$$

ou $$(A - a^2)\,x = 2a,$$

ce qui donne

$$\left.\begin{aligned} a &= ex, \\ A &= a^2 + 2e, \\ \sqrt{A} &= a\,(x,\ 2a)\ (^1). \end{aligned}\right\} \quad (2)$$

On est aussi amené à considérer deux cas :

1° x pair alors $\sqrt{e^2x^2 + e} = ex\,(2x,\ 2ex)$.

2° x impair alors $\sqrt{e^2x^2 + 2e} = ex\,(x,\ 2ex)$.

On peut diminuer la généralité de ces formules et se donner la valeur de x, on aura, par exemple

$$\sqrt{e^2 + 2e} = e\,(1,\ 2e), \qquad \text{en faisant} \qquad x = 1,$$

$$\sqrt{e^2 + e} = e\,(2,\ 2e),$$

$$\sqrt{x^2 + 2} = x\,(x,\ 2x), \qquad e = 1.$$

---

(1) Dans certaines questions on est amené à étudier les fractions continues générales

$$x = a_0 + \frac{a_1}{b_1} + \frac{a_2}{b_2} + \frac{a_3}{b_3} + \cdots,$$

que nous écrirons en abrégé

$$x = a_0, \quad \frac{a_1}{b_1}, \quad \frac{a_2}{b_2}, \quad \ldots.$$

La loi de formation des réduites est

$$p_{k+1} = p_k\, b_k + p_{k-1}\, a_{k-1},$$

$$q_{k+1} = q_k\, b_k + q_{k-1}\, a_{k-1}.$$

Si on pose $\qquad A = a^2 + b\ (b \leqslant 2a),$

on trouve $\qquad \sqrt{A} = a, \quad \frac{b}{2a}, \quad \frac{b}{2a}, \quad \frac{b}{2a}, \quad \ldots.$

Cette formule donne (1) quand on y fait $b = 1$.

Si on pose $2a = bx$, on trouve

$$\sqrt{A} = a, \quad \frac{b}{2a}, \quad \frac{b}{2a}, \quad \frac{b}{2a}, \quad \ldots,$$

qu'on transforme facilement en (2)

$$\sqrt{A} = a\,(x,\ 2a).$$

On trouvera ainsi le développement de $\sqrt{A}$ pour

A = 3, 6, 8, 11, 12, 15, 18, 20, 24, 27, 30, 35, 38, 39, 40, 42, 48, 51, 56, 63, 66, 68, 72, 80, 83, 84, 87, 90, 99, 102, 104, 105, 110, 120, 123, 132, 143, 146, 147, 148, 150, 152, 156, 168, 171, 182, 195, 198, 200, 203, 210, 224, 227, 228, 230, 231, 235, 240, 255, 258, 260, 264, 272, 288, 291, 306, 323, 326, 327, 328, 330, 333, 336, 342, 360, 363, 380, 399, 402, 404, 405, 408, 410, 420, 440, 443, 444, 447, 448, 455, 462, 483, 486, 488, 495, 506, 528, 531, 552, 575, 578, 579, 580, 582, 584 588, 592, 600, 624, 627, 630, 635, 650, 675, 678, 680, 689, 702, 728, 731, 732, 735, 738, 747, 756, 783, 786, 788, 791, 792, 798, 812, 840, 843, 870, 899, 902, 903, 904, 905, 906, 910, 912, 915, 920, 930, 960, 963, 992, ..., etc.

5. Il peut arriver que la période soit constituée par deux termes dans la partie symétrique.

Soit
$$\sqrt{A} = a\,(x, x, 2a),$$

ou

$$\sqrt{A} - a = 0, x, x, \sqrt{A} + a = \begin{array}{c|c|c|c} & & x & \sqrt{A} + a \\ \hline 0 & 1 & x & x\,(\sqrt{A} + a) + 1 \\ \hline 1 & x & x^2 + 1 & (x^2 + 1)(\sqrt{A} + a) + x \end{array}$$

ou
$$(A - a^2)(x^2 + 1) = 2a\,x + 1.$$

Cette équation n'est pas possible si x est impair.

Dans le cas contraire, on aura

$$\left.\begin{aligned} 2a &= x + 2\,(x^2 + 1)\,e, \\ A &= a^2 + 1 + 2xe, \\ \sqrt{A} &= a\,(x, x, 2a). \end{aligned}\right\} \quad (3)$$

On trouve $\quad 4A = (x + 2x^2e - 2e)^2 + (2 + 4ex)^2.$

Sous la réserve que x sera pair les formules (3) déterminent toujours un développement.

On peut fixer la valeur de x.

Ainsi $x = 4$ donne

$$A = (17e + 2)^2 + (8e + 1) = (15e + 2)^2 + (8e + 1)^2,$$

$$\sqrt{A} = 17e + 2\,(4,\ 4,\ 34e + 4).\ (^1)$$

On trouvera ainsi le développement de $\sqrt{A}$ pour les valeurs suivantes de A

$$A = 41,\ 130,\ 269,\ 370,\ 458,\ 697,\ 986,\ \text{etc.},$$

pour lesquels on a respectivement

$$x = 2,\ 2,\ 2,\ 4,\ 2,\ 2,\ 2.$$

6. On peut avoir trois termes dans la partie symétrique de la période. On aura alors un développement de la forme

$$\sqrt{A} = (x,\ y,\ x,\ 2a),$$

ce qui donne

$$\sqrt{A} - a = 0,\ x,\ y,\ x,\ \sqrt{A} + a$$

		y	x	$\sqrt{A} + a$
$=$ 0	1	y	$xy + 1$	$(xy + 1)(\sqrt{A} + a) + y$
1	x	$xy + 1$	$x^2y + 2x$	$(x^2y + 2x)(\sqrt{A} + a) + (xy + 1)$

On en tire

$$(A - a^2)(x^2y + 2x) = 2a\,(xy + 1) + y.$$

---

(1) Si on pose

$$A = \frac{1}{17^2}(2^{68} + 1) = 1021273028302258913.$$

On trouve

$$\sqrt{A} = a\,(4,\ 4,\ 2a)$$

étant posé

$$a = 1010580540,$$

par conséquent

$$A = (15e + 2)^2 + (8e + 1)^2$$

e étant déterminé par la relation

$$17e + 2 = a \qquad \text{d'où} \qquad A = 8916887 12^2 + 475567313^2.$$

Nous rencontrerons plus loin ce développement.

Cette équation montre que si y est impair x ne peut pas être pair, car, dans le cas contraire, le premier membre sera pair et le deuxième impair.

Les réduites de $\sqrt{A}$ donnent l'identité

$$(x^2y + 2x)\, y = (xy + 1)^2 - 1,$$

ou

$$(x^2y + 2x)\, y^2 = (xy + 1)^2\, y - y.$$

On aura ainsi

$$\left.\begin{aligned} 2a &= -(xy + 1)\, y + (x^2y + 2x)\, e, \\ A &= a^2 - y^2 + (xy + 1)\, e, \\ \sqrt{A} &= a\,(x, y, x, 2a). \end{aligned}\right\} \quad (4)$$

Ces formules sont triplement indéterminées, car x, y et e sont arbitraires. On peut donc les préciser en se donnant soit la valeur de x, soit celle de y, ou les deux.

Le seul cas à ne pas considérer est celui quand y est impair et x pair.

Voici quelques-uns des résultats qu'on obtient ainsi :

1° Soit $x = 1$, on trouvera une série de formules doublement indéterminées (y et e étant arbitraires) pour le développement de la forme

$$\sqrt{A} = a\,(1,\ y,\ 1,\ 2a).$$

Il sera commode de les subdiviser en deux groupes suivant que y est pair ou impair.

Retenons, en particulier, le résultat obtenu en faisant dans (4)

$$x = 1, \qquad y = e - 1.$$

On trouve

$$a = e, \qquad A = e^2 + 2e - 1,$$

d'où

$$\sqrt{e^2 + 2e - 1} = e\,(1,\ e - 1,\ 1,\ 2e,$$

ou bien

$$\sqrt{f^2 - 2} = f - 1\,(1,\ f - 2,\ 1,\ 2f - 2),$$

étant posé

$$e = f - 1.$$

Cette dernière fait partie comme cas particulier des formules générales suivantes

$$\sqrt{(2e+1)^2 a^2 - 2a} = (2e+1)\,a - 1\,[1, 2e-1, 1, 2(2e+1)\,a - 2],$$

$$\sqrt{e^2a^2 - a} = ea - 1\,(1,\ 2e-2,\ 1,\ 2ea-2),$$

qu'on peut avantageusement comparer avec celles que nous avons obtenues dans le cas, quand la période est constituée d'un seul terme dans la partie périodique (n° 4, p. 31-33).

2° On peut prendre $x = 2$, alors y doit être pair, posons $y = 2z$ et on trouvera une formule contenant les deux paramètres e et z, susceptible d'ailleurs de simplifications sur lesquelles nous n'insistons pas.

3° Posons $x = 3$. On trouve

$$2a = -(3y+1)\,y + (9y+6)\,e,$$

$$A = a^2 - y^2 + (3y+1)\,e.$$

Ces formules se simplifient, si on pose

$$y = 3f + 2, \qquad e = f + 1,$$

il vient

$$a = 6f + 5, \qquad A = (6f+5)^2 + (4f+3),$$

$$\sqrt{A} = a\,(3,\ 3f+2,\ 3,\ 2a).$$

4° On trouve des simplifications analogues à 2° avec $x = 4$, 6, 8, ..., etc.

5° Posons $x = 5$. On trouvera une infinité de formules à deux paramètres y et e dont la suivante est à retenir.

Si on fait ($x = 5$), $y = 5f + 2$, $e = f + 1$, il vient

$$\sqrt{(40f+19)^2 + (16f+7)} = 40f + 19\,(5,\ 5f+2,\ 5,\ 80f+38).$$

6° Posons $x = 7$, $y = 7f + 2$, il vient (avec $e = f + 1$)

$$\sqrt{(126f+41)^2 + (36f+11)} = 126f + 41\,(7, 7f+2, 7, 252f+82).$$

Ces formules sont les plus simples parmi celles qui correspondent à un développement dont la partie symétrique de la période contient trois termes.

Si ces trois termes sont

$$2g + 1, \qquad (2g + 1)\,h + 2, \qquad 2g + 1,$$

la formule correspondante est sensiblement plus simple que dans le cas général.

On trouve ainsi le développement de $\sqrt{A}$ pour les valeurs suivantes de A.

A	x	y	A	x	y	A	x	y	A	x	y	A	x	y	A	x	y
7	1	1	136	1	1	254	1	14	398	1	18	615	1	3	795	5	9
14	1	2	138	1	2	266	3	4	427	1	1	620	1	8	799	3	1
23	1	3	140	1	4	287	1	15	434	1	4	623	1	23	839	1	27
28	3	2	141	1	6	299	3	2	435	1	5	632	7	6	850	6	2
32	1	1	142	1	10	300	3	8	438	1	12	646	2	2	855	4	6
33	1	2	155	2	4	305	2	6	439	1	19	663	1	2	858	3	2
34	1	4	167	1	11	312	1	1	473	1	2	672	1	11	860	3	14
47	1	5	174	5	4	315	1	2	480	1	9	674	1	24	880	1	1
55	2	2	176	3	1	318	1	4	482	1	20	711	1	1	885	1	2
60	1	2	180	2	2	320	1	7	504	2	4	720	1	4	888	1	3
62	1	6	189	1	2	321	1	10	505	2	8	723	1	7	890	1	4
75	1	1	192	1	5	322	1	16	527	1	21	726	1	16	894	1	8
78	1	4	194	1	12	335	3	3	544	3	11	727	1	25	895	1	10
79	1	7	215	1	1	359	1	17	560	1	1	755	2	10	896	1	13
95	1	2	219	1	3	368	5	2	564	1	2	770	1	2	897	1	18
96	1	3	220	1	4	377	2	2	568	1	4	776	1	5	898	1	28
98	1	8	222	1	8	390	1	2	570	1	6	777	1	6	959	1	29
119	1	9	223	1	13	392	1	3	572	1	10	780	1	12	975	4	2
126	4	2	248	1	2	395	1	6	573	1	14	782	1	26	987	2	2
128	3	5	252	1	6	396	1	8	574	1	22	793	6	4	990	2	6

7. On peut avoir quatre termes dans la partie symétrique.

On aura alors un développement de la forme

$$\sqrt{A} = a\,(x,\ y,\ y,\ x,\ 2a).$$

Nous démontrerons d'abord qu'il n'est pas possible que x soit impair et y pair, car on trouve

$$\sqrt{A} - a = 0,\ x,\ y,\ y,\ x,\ \sqrt{A} + a$$

		y	y	x	$\sqrt{A} + a$
$= 0$	1	y	$y^2 + 1$	$y^2x + x + y$	$(xy^2 + x + y)$ $(\sqrt{A} + a) + y^2 + 1$
1	x	$xy + 1$	$xy^2 + y + x$	$x^2y^2 + 2xy$ $+ x^2 + 1$	$(x^2y^2 + 2xy + x^2 + 1)$ $(\sqrt{A} + a) + xy^2 + y + x$

On aura ainsi l'équation

$$(A - a^2)(x^2y^2 + 2xy + x^2 + 1) = 2a\,(xy^2 + x + y) + y^2 + 1. \quad (1)$$

Si on suppose que x est impair et y pair, le premier membre est pair et le second impair et l'équation (1) sera impossible.

On aura ainsi à envisager les trois cas suivants :

1° x impair, y impair,

2° x pair, y impair,

3° x pair, y pair.

Des réduites de $\sqrt{A}$ résulte l'identité

$$(x^2y^2 + 2xy + x^2 + 1)(y^2 + 1) - (xy^2 + x + y)^2 = 1,$$

ou

$$(x^2y^2 + 2xy + x^2 + 1)(y^2 + 1)^2 = (xy^2 + x + y)^2(y^2 + 1) + (y^2 + 1)^2,$$

cette identité comparée avec l'équation (1) donne

$$\left.\begin{aligned} 2a &= (y^2 + 1)(xy^2 + x + y) + 2\,(x^2y^2 + 2xy + x^2 + 1)\,e, \\ A &= a^2 + (y^2 + 1)^2 + 2\,(xy^2 + x + y)\,e, \\ \sqrt{A} &= a\,(x,\ y,\ y,\ x,\ 2a). \end{aligned}\right\} (5)$$

Comme dans (3) A peut être mis sous la forme $A = m^2 + n^2$.

Ces formules déterminent une solution sauf quand x est impair et y pair.

On aura une multiple infinité de cas particuliers en précisant les valeurs de x, y et e, ou de l'une, ou de deux de ces quantités.

Par exemple $x = 2$, $y = 1$, donne

$$a = 13e + 5, \quad A = (13e + 5)^2 + 4 + 10e = (12e + 5)^2 + (5e + 2)^2,$$

$$\sqrt{A} = 13e + 5\,(2,\ 1,\ 1,\ 2,\ (26e + 10).$$

On trouve ainsi le développement de $\sqrt{A}$ pour

A	x	y	A	x	y	A	x	y	A	x	y	A	x	y	A	x	y
13	1	1	89	2	3	229	7	1	373	3	5	701	2	10	925	2	2
29	2	1	125	5	1	293	8	1	445	10	1	733	13	1	965	15	1
53	3	1	173	6	1	338	2	1	533	11	1	818	1	1	985	2	1
74	1	1	185	1	1	346	1	1	557	1	1	845	14	1			
85	4	1	218	1	3	365	9	1	629	12	1	914	4	3			

On peut se proposer de trouver la formule générale (5) en y faisant $y = 1$, comme cela a lieu pour vingt-deux des valeurs considérées de A.

Les formules (5) deviennent

$$2a = 2\,(2x + 1) + 2\,(2x^2 + 2x + 1)\,e,$$

$$A = a^2 + 4 + 2\,(2x + 1)\,e,$$

ou bien

$$a = (2x + 1) + (2x^2 + 2x + 1)\,e,$$

$$A = a^2 + 2\,(2x + 1)\,e + 4$$

$$= [(2x^2 + 2x + 1)\,e + (2x + 1)]^2 + 2\,(2x + 1)\,e + 4$$

$$= [(2x^2 + 2x)\,e + (2x + 1)]^2 + [(2x + 1)\,e + 2]^2.$$

On aura alors

$$\sqrt{A} = a\,(x,\ 1,\ 1,\ x,\ 2a.$$

8. Il peut arriver que la période soit constituée de cinq termes dans la partie symétrique. On aura alors

$$\sqrt{A} = a\,(x,\ y,\ z,\ y,\ x,\ 2a),$$

ou

$$\sqrt{A} - a = 0,\ x,\ y,\ z,\ y,\ x,\ \sqrt{A} + a$$

$$= \begin{array}{c|c|c|c|c|c|c}
 & & y & z & y & x & \sqrt{A} + a \\
\hline
0 & 1 & y & zy + 1 & zy + 2y = R & \begin{array}{c} xzy^2 + 2xy \\ + zy + 1 = P \end{array} & \begin{array}{c} P(\sqrt{A} + a) \\ + zy^2 + 2y \end{array} \\
\hline
1 & x & xy + 1 & xyz + z + x & \begin{array}{c} xy^2z + zy \\ + 2xy + 1 \end{array} & \begin{array}{c} x^2y^2z + 2xzy \\ + 2x^2y + 2x \\ + z = Q \end{array} & Q(\sqrt{A} + a) + P
\end{array}$$

On aura ainsi l'équation

$$(A - a^2)(x^2y^2z + 2xzy + 2x^2y + 2x + z)$$
$$= 2a\,(xzy^2 + 2xy + zy + 1) + zy^2 + 2y,$$

ou avec nos notations

$$(A - a^2)\,Q = 2aP + zy^2 + 2y.$$

Or

$$Q\,(zy^2 + 2y) - P^2 = -1,$$

ou

$$Q\,(zy^2 + 2y)^2 = P^2\,(zy^2 + 2y) - (zy^2 + 2y),$$

d'où

$$\left.\begin{aligned} 2a &= -P\,(zy^2 + 2y) + Qe, \\ A &= a^2 - (zy^2 + 2y)^2 + Pe, \\ \sqrt{A} &= a\,(x,\ y,\ z,\ y,\ x,\ 2a), \end{aligned}\right\} \quad (6)$$

en posant

$$Q = x^2y^2z + 2xzy + 2x^2y + 2x + z,$$
$$P = xzy^2 + 2xy + zy + 1.$$

Ces formules contiennent quatre paramètres (x, y, z et a). On peut les rendre moins générales en précisant certaines de ces quantités. Par exemple $x = y = 1$, $z = 2$, donne

$$R = 4,\quad P = 2 + 2 + 2 + 1 = 7,\quad Q = 2 + 4 + 2 + 2 + 2 = 12,$$

$$2a = -28 + 12e, \qquad \text{ou} \qquad a = 6e - 14.$$

$$A = (6e - 14)^2 + (7e - 16),$$

$$\sqrt{A} = 6e - 14\,(1,\ 1,\ 2,\ 1,\ 1,\ 12e - 28).$$

Le seul cas qu'il ne faut pas considérer est celui qui rend R et P impair et Q pair, car alors a est fractionnaire. Sous cette réserve toutes les valeurs de x, y, z conduisent à une solution entière.

On obtient ainsi le développement de $\sqrt{A}$ pour les valeurs suivantes de A

A	x	y	z	A	x	y	z	A	x	y	z	A	x	y	z	A	x	y	z
19	2	1	2	175	4	2	1	350	1	2	2	525	1	10	2	740	4	1	12
21	1	1	2	178	2	1	12	357	1	8	2	545	2	1	8	759	1	1	4
22	1	2	4	183	1	1	8	371	3	1	4	546	2	1	2	803	2	1	27
45	1	1	2	187	1	2	13	372	3	2	12	551	2	8	1	813	1	1	1
52	4	1	2	208	2	2	1	374	2	1	18	567	1	4	3	817	1	1	2
54	2	1	6	216	1	2	3	381	1	1	12	590	3	3	4	822	1	2	28
57	1	1	4	221	1	6	2	387	1	2	19	602	1	1	6	828	1	3	2
59	1	2	7	232	4	3	7	407	5	1	2	618	1	6	8	837	1	13	2
70	2	1	2	267	2	1	15	418	2	4	20	621	1	11	2	848	8	3	3
77	1	3	2	270	2	3	6	437	1	9	2	642	2	1	24	867	2	4	29
88	2	1	1	273	1	1	10	456	2	1	4	648	2	5	6	923	2	1	1
107	2	1	9	275	1	1	2	470	1	2	8	649	1	2	25	943	1	2	2
111	1	1	6	278	1	2	16	498	3	6	12	651	1	1	16	957	1	14	2
112	1	1	2	280	1	2	1	499	2	1	21	659	1	2	25	966	12	2	2
114	1	2	10	285	1	7	2	507	1	1	14	660	1	2	4	968	8	1	6
117	1	4	2	294	6	1	4	510	1	1	2	690	3	1	2	982	2	1	30
131	2	4	11	296	6	1	4	514	1	2	24	700	2	5	2	993	1	1	20
164	1	4	6	303	2	2	5	518	1	3	6	712	1	2	6	994	1	1	6
165	1	5	2	308	1	1	4	520	1	4	11	725	1	12	1				

Les formules particulières suivantes sont à retenir

$$\sqrt{(3e+1)^2+(4e+2)} = 3e+1\ (1,\ 2,\ 3e+1,\ 2,\ 1,\ 6e+2),$$

$$\sqrt{(3e+1)^2+(2e+1)} = 3e+1\ (2,\ 1,\ \ 3e,\ \ 1,\ 2,\ 6e+2),$$

$$\sqrt{(9e+2)^2+(8e+2)} = 9e+2\ (2,\ 4,\ 9e+2,\ 4,\ 2,\ 18e+4).$$

9. On aura six termes dans la partie symétrique de la période si on a

$$\sqrt{A} = a\,(x,\ y,\ z,\ z,\ y,\ x,\ 2a),$$

ou

$$\sqrt{A} - a = 0,\ x,\ y,\ z,\ z,\ y,\ x,\ \sqrt{A} + a$$

		y	z	z	y	x	$\sqrt{A} + a$
0	1	y	$yz + 1$	$yz^2 + z + y$	R	P	$P(\sqrt{A} + a) + R$
1	x	$yx + 1$	$xyz + z + x$	$xy^2z + z^2 + xz + xy + 1$	P	Q	$Q(\sqrt{A} + a) + P$

étant posé

$$R = y^2z^2 + 2yz + y^2 + 1,$$

$$P = xy^2z^2 + 2xyz + yz^2 + x + yz^2 + y + z,$$

$$Q = x^2y^2z^2 + z^2xy + 2x^2yz + x^2y^2 + 2xy + 2xz + x^2 + xyz^2 + z^2 + 1.$$

On aura ainsi

$$\sqrt{A} - a = \frac{P(\sqrt{A} + a) + R}{Q(\sqrt{A} + a) + P},$$

ou

$$(A - a^2)\,Q = 2aP + R,$$

or

$$\frac{P}{Q} - \frac{R}{P} = \frac{-1}{QP},$$

ou

$$QR - P^2 = 1,$$

ou

$$QR^2 = P^2R + R,$$

d'où

$$\left.\begin{aligned} 2a &= PR + Qe, \\ A &= a^2 + R^2 + Pe, \\ \sqrt{A} &= a\,(x,\ y,\ z,\ z,\ y,\ x,\ 2a). \end{aligned}\right\} \quad (7)$$

Dans ce cas encore, A est une somme de deux carrés.

Voici les développements (pour A < 1000) dont la partie symétrique de la période est constituée de six termes.

A	Partie entière	Période						
		Partie symétrique						Dernier terme
58	7	1	1	1	1	1	1	14
73	8	1	1	5	5	1	1	16
250	15	1	4	3	3	4	1	30
274	16	1	1	4	4	1	1	32
314	17	1	2	1	1	2	1	34
349	18	1	2	7	7	2	1	36
425	20	1	1	1	1	1	1	40
538	23	5	7	1	1	7	5	46
761	27	1	1	2	2	1	1	54

NOTE.— On obtient deux fois (A = 58 et A = 425) la période 1, 1, 1, 1, 1, 1. Voyons, dans quel cas obtient-on cette période.

Posons

$$\sqrt{A} = x\,(1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 2x),$$

ou

$$\sqrt{A} - x = 0,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ \sqrt{A} + x,$$

ou

$$\sqrt{A} - x = \frac{0}{1},\ \frac{1}{1},\ \frac{1}{2},\ \frac{2}{3},\ \frac{3}{5},\ \frac{5}{8},\ \frac{8}{13},\ \frac{8\,(\sqrt{A} + x) + 5}{13\,(\sqrt{A} + x) + 8},$$

d'où

$$13\,(A - x^2) = 16x + 5.$$

Pour que $16x + 5$ soit divisible par 13, il faut qu'on ait

$$x = 13e + 7.$$

Avec cette valeur de e, on trouve

$$\begin{aligned} A &= x^2 + 16e + 9 = (13e + 7)^2 + (16e + 9) \\ &= (12e + 7)^2 + (5e + 3)^2, \end{aligned}$$

$$e = 0 \quad \text{donne} \quad A = 58,$$

$$e = 1 \quad \text{»} \quad A = 425.$$

10. Soit, en général, une période constituée de $k + 1$ termes dont k de la partie symétrique sont fonctions de $\frac{k}{2}$ ou $\frac{k+1}{2}$ paramètres suivant que k est pair ou impair.

On aura ainsi

$$\sqrt{A} = a\,(x, y, z, t, \ldots, t, z, y, x, 2a).$$

Soit $\frac{R}{P}$ et $\frac{P}{Q}$ les réduites de la fraction

$$\sqrt{A} = a = 0, x, y, z, t, \ldots, \sqrt{A} + a,$$

qui correspondent aux quotients incomplets y et x finissant la partie symétrique de la période. On aura

$$\sqrt{A} - a = \frac{P(\sqrt{A} + a) + R}{Q(\sqrt{A} + a) + P},$$

ou

$$(A - a^2)\,Q = 2aP + R.$$

Cette équation montre que si Q est pair et R impair l'équation n'est pas possible. Ainsi certaines périodes ne sont pas possibles. Par exemple, les périodes, dont la partie symétrique est composée de

Deux termes	$2x + 1,\ 2x + 1,$
Trois »	$2x,\ 2y + 1,\ 2x,$
Quatre »	$2x + 1,\ 2y,\ 2y,\ 2x + 1,$

ne sont pas possibles.

Dans les autres cas, on aura

$$QR = P^2 \pm 1, \qquad \text{ou} \qquad QR^2 = P^2R \pm R,$$

ce qui donne

$$\left.\begin{aligned} 2a &= \pm PR + Qe, \\ A &= a^2 \pm R^2 + Pe. \end{aligned}\right\} \quad (8)$$

On aura ainsi une formule renfermant $\left(\frac{k}{2} + 1\right)$ ou $\left(\frac{k+1}{2} + 1\right)$ paramètres : $x, y, z, \ldots$ et e.

12. Ainsi pour un développement quelconque renfermant dans la partie symétrique $2k - 1$ ou $2k$ termes, on trouve des formules contenant $k + 1$ paramètres : $x, y, z, \ldots$ et e.

Parmi ces formules il y en a une

$$2a = \pm PR + Qe.$$

qui montre que certains développements ne sont pas possibles,

à savoir, ceux dans lesquels Q est pair et R impair (si Q est pair P est impair puisque $\frac{P}{Q}$ est irréductible). Ces cas étant exclus, les équations (8) sont toujours possibles.

Les quantités x, y, z, . . ., e sont quelconques et tant que toutes ces quantités sont indéterminées, on a des formules dont le degré d'indétermination est $k+1$.

On aura donc encore des formules indéterminées en précisant certaines de ces quantités.

Voici les développements de $\sqrt{A}$ conduisant à une période contenant sept termes dans la partie périodique.

Pour abréger, on n'écrit que la moitié de la période, le dernier terme écrit étant celui du milieu de la partie symétrique. Pour avoir la partie symétrique en entier, il faut ajouter les trois premiers termes écrits dans l'ordre inverse. Le dernier terme de la période n'est pas écrit non plus, il est $2a$. Enfin, pour avoir le développement complet, il faut encore ajouter la partie entière a.

Exemple $\sqrt{31} = 5\,(1, 1, 3, 5, 3, 1, 1, 10)$.

A	Période				A	Période				A	Période				A	Période			
31	1	1	3	5	316	1	3	2	8	638	3	1	6	2	868	2	6	19	2
44	1	1	1	2	332	4	1	1	8	658	1	1	1	6	874	1	1	3	2
69	3	3	1	4	348	1	1	1	8	668	1	5	2	12	876	1	1	2	14
71	2	2	1	7	352	1	3	5	9	684	6	1	1	12	882	1	2	3	6
91	1	1	5	1	378	2	3	1	4	693	3	12	1	4	884	1	2	1	2
92	1	1	2	4	383	1	1	3	19	695	2	1	3	10	891	1	5	1	1
108	2	1	1	4	384	1	1	2	9	696	2	1	1	1	892	1	6	2	14
135	1	1	1	1	413	3	9	1	4	704	1	1	7	13	908	7	1	1	14
153	2	1	2	2	414	2	1	7	2	706	1	1	3	26	909	6	1	2	6
158	1	1	3	12	416	2	1	1	9	707	1	1	2	3	924	2	1	1	14
160	1	1	1	5	423	1	1	3	4	710	1	1	1	4	927	2	5	5	3
177	3	3	2	8	432	1	3	1	1	736	7	1	2	1	933	1	1	5	20
188	1	2	2	6	450	4	1	2	4	743	3	1	7	27	935	1	1	2	1
202	4	1	2	2	468	1	1	1	2	752	2	2	1	2	936	1	1	2	6
204	3	1	1	6	476	1	4	2	10	768	1	2	2	13	939	1	1	4	20
205	3	6	1	4	492	5	1	1	10	800	3	1	1	13	940	1	1	1	14
206	2	1	5	14	503	2	2	1	21	808	2	2	1	4	942	1	2	4	20
207	2	1	1	2	539	4	4	1	1	810	2	5	1	4	952	1	5	1	6
209	2	5	3	2	540	4	4	1	10	814	1	1	7	2	973	5	5	2	8
234	3	2	1	2	555	1	1	3	1	816	1	1	3	3	983	2	1	5	31
238	2	2	1	14	585	5	2	1	4	852	5	3	2	4					
279	1	2	2	1	608	1	1	1	11	854	4	2	11	4					
282	1	3	1	4	612	1	2	1	4	866	2	2	1	28					

Certains de ces développements sont à noter :

1° Voyons d'abord dans quel cas la partie symétrique de la période est-elle 1, 1, 1, x, 1, 1, 1 ?

Posons

$$\sqrt{A} - a = 0, 1. 1, 1, x, 1, 1, 1, \sqrt{A} + a.$$

			1	1	x	1	1	1	$\sqrt{A}+a$
$\sqrt{A}-a=$	0	1	1	2	$2x+1$	$2x+3$	$4x+4$	$6x+7$	$(6x+7)(\sqrt{A}+a)$ $+4x+4$
	1	1	2	3	$3x+2$	$3x+5$	$6x+7$	$9x+12$	$(9x+12)(\sqrt{A}+a)$ $+(6x+7)$

On aura ainsi

$$(A - a^2)(9x + 12) = 2a\,(6x + 7) + 4x + 4.$$

Or

$$(9x + 12)(4x + 4) - (6x + 7)^2 = -1,$$

ou

$$(9x + 12)(4x + 4)^2 = (6x + 7)^2\,(4x + 4) - (4x + 4),$$

d'où

$$\left.\begin{aligned} a &= -(6x + 7)(2x + 2) + (9x + 12)\,e, \\ A &= a^2 - (4x + 4)^2 + 2\,(6x + 7)\,e, \end{aligned}\right\}$$

on aura ainsi

$$\sqrt{A} = a\,(1, 1, 1, x, 1, 1, 1, 2a).$$

On trouvera comme cas particuliers les développements de $\sqrt{A}$ pour A = 44, 135, 160, 348, 468, 608, 658, 710, etc.

2° Les développements de $\sqrt{A}$ pour A = 71, 238, 503, 866 conduisent à poser

$$\sqrt{A} = a\,(2, 2, 1, a-1, 1, 2, 2, 2a),$$

ou

$$\sqrt{A} - a = 0, 2, 2, 1, a - 1, 1, 2, 2, \sqrt{A} + a,$$

			2	1	$a-1$	1	2	2	$\sqrt{A}+a$
$\sqrt{A}-a=$	0	1	2	3	$3a-1$	$3a+2$	$9a+3$	$21a+8$	$(21a+8)(\sqrt{A}+a)$ $+(9a+3)$
	1	2	5	7	$7a-2$	$7a+5$	$21a+8$	$49a+21$	$(49a+21)(\sqrt{A}+a)$ $+(21a+8)$

$$(A - a^2)(49a + 21) = 2a\,(21a + 8) + 9a + 3 = 42a^2 + 25a + 3,$$

faisons $a = 7e + 1$, il vient

$$(A - a^2)(49e + 10) = (294e^2 + 109e + 10).$$

$$A = a^2 + 6e + 1 = (7e + 1)^2 + (6e + 1),$$

et on aura

$$\sqrt{(7e+1)^2 + (6e+1)} = 7e + 1\,(2,\ 2,\ 1,\ 7e,\ 1,\ 2,\ 2,\ 14e + 2).$$

3° Les développements de $\sqrt{A}$ pour $A = 31,\ 706$ conduisent à poser

$$\sqrt{A} = a\,(1,\ 1,\ 3,\ a,\ 3,\ 1,\ 1,\ 2a),$$

			1	3	a	4	1	1	$\sqrt{A} + a$
$\sqrt{A} - a =$	0	1	1	4	$4a+1$	$12a+7$	$16a+8$	$28a+15$	$(28a+15)(\sqrt{A}+a) + (16a+8)$
	1	1	2	7	$7a+2$	$21a+13$	$28a+15$	$49a+28$	$(49a+28)(\sqrt{A}+a) + (28a+15)$

$$(A - a^2)(49a + 28) = 2a\,(28a + 15) + (16a + 8).$$

En posant $a = 7e + 5$, il vient

$$A = (7e + 5)^2 + (8e + 6),$$

donnant le développement de $\sqrt{A}$ pour $A = 31,\ 158,\ 383,\ 706$ avec $e = 0,\ 1,\ 2,\ 3$.

4° On peut préciser tous les termes d'un développement.

Par exemple le développement

$$\sqrt{A} = a\,(1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 2a),$$

donne

			1	1	1	1	1	1	$\sqrt{A} + a$
$\sqrt{A} - a =$	0	1	1	2	3	5	8	13	$13\,(\sqrt{A} + a) + 8$
	1	1	2	3	5	8	13	21	$21\,(\sqrt{A} + a) + 13$

d'où

$$(A - a^2)\,21 = 26a + 8,$$

ce qui conduit à poser

$$a = 21e + 11,$$

et on aura

$$A = a^2 + 26e + 14,$$

d'où

$$\sqrt{(21e+11)^2 + (26e+14)} = (21e+11)(1, 1, 1, 1, 1, 1, 1, (42e+22).$$

12. Les valeurs suivantes de A sont telles que le développement de $\sqrt{A}$ conduit à une période dont la partie symétrique contient huit termes.

A	a	S								$2a$
106	10	3	2	1	1	1	1	2	3	20
113	10	1	1	1	2	2	1	1	1	20
137	11	1	2	2	1	1	2	2	1	22
149	12	4	1	5	3	3	5	1	4	24
265	16	3	1	1	2	2	1	1	3	32
389	19	1	2	1	1	1	1	2	1	38
493	22	4	1	10	3	3	10	1	4	44
610	24	1	2	3	5	5	3	2	1	48
698	26	2	2	1	1	1	1	2	2	52
754	27	2	5	1	1	1	1	5	2	54
970	31	6	1	9	1	1	9	1	6	62

Chacune de ces formules peut conduire à une formule générale contenant un, deux, trois, quatre ou cinq paramètres.

Ainsi le développement de $\sqrt{A}$ pour $A = 113$ conduit à la formule

$$\sqrt{(73e+10)^2 + (92e+13)} = 73e+10\,(1, 1, 1, 2, 2, 1, 1, 1, 146e+20).$$

On remarquera que

$$A = (73e+10)^2 + (92e+13),$$

est une somme de deux carrés

$$A = (55e+8)^2 + (48e+7)^2.$$

13. Voici les développements qui contiennent dans la partie symétrique de la période neuf termes. La table qui suit donne

les cinq premiers termes de la période. Pour achever la période il faut ajouter à la suite des cinq premiers termes les quatre premiers écrits dans l'ordre inverse. De plus, il faut écrire dans la période le dernier terme $2a$, et ajouter la partie entière a.

Exemple $\sqrt{43} = 6\,(1,\ 1,\ 3,\ 1,\ 5,\ 1,\ 3,\ 1,\ 1,\ 12)$.

A	Période					A	Période					A	Période					A	Période				
43	1	1	3	1	5	339	2	2	2	1	7	534	9	4	1	1	22	741	4	1	1	13	18
67	5	2	1	1	7	344	1	1	4	1	3	536	6	1	1	2	5	744	3	1	1	1	1
86	3	1	1	1	8	345	1	1	2	1	6	543	3	3	3	1	14	760	1	1	3	5	1
93	1	1	1	4	6	354	1	4	2	2	18	563	1	2	1	2	23	762	1	1	1	1	8
115	1	2	1	1	1	375	2	1	2	1	5	583	6	1	7	5	4	765	1	1	1	13	6
116	1	3	1	4	1	403	13	2	1	3	1	591	3	4	1	1	7	774	1	4	1	1	2
118	1	6	3	2	10	411	3	1	1	1	19	594	2	1	2	5	24	779	1	10	5	2	27
129	2	1	3	1	6	451	4	4	2	8	21	595	2	1	1	4	1	804	2	1	4	2	18
154	2	2	3	1	2	452	3	1	5	3	10	598	2	4	1	15	2	819	1	1	1	1	1
159	1	1	1	1	3	453	3	1	1	10	14	603	1	1	3	1	23	827	1	3	7	1	27
161	1	2	4	1	2	459	2	2	1	4	21	616	1	4	1	1	6	830	1	4	3	1	10
162	1	2	1	2	12	464	1	1	5	1	1	644	2	1	1	1	6	836	1	10	1	1	2
186	1	1	1	3	4	465	1	1	3	2	2	645	2	1	1	12	10	847	9	1	2	6	8
237	2	1	1	7	10	469	1	1	1	10	6	656	1	1	1	1	2	872	1	1	7	1	13
242	1	1	3	1	14	475	1	3	1	6	2	665	1	3	1	2	2	918	3	2	1	6	30
243	1	1	2	3	15	490	7	2	1	4	4	671	1	9	2	1	1	938	1	1	1	2	8
245	1	1	1	7	6	494	4	2	2	1	2	682	8	1	2	5	2	945	1	2	1	6	12
246	1	2	5	1	14	497	3	2	2	5	6	687	4	1	2	1	16	948	1	3	1	3	20
259	10	1	2	3	4	515	1	2	3	1	3	703	1	1	17	5	1	978	3	1	1	1	30
286	1	10	3	3	2	516	1	2	1	1	14	705	1	1	4	3	10	979	3	2	5	1	4
292	11	2	1	3	8	522	1	5	1	1	4	714	1	2	1	1	2	980	3	3	1	1	2
297	4	3	1	1	2	532	15	2	1	4	2	715	1	2	1	5	5	984	2	1	2	2	7

Chacun de ces développements peut être généralisé.

Ainsi le développement de $\sqrt{43}$ conduit à la formule générale suivante

$$\sqrt{(9e+6)^2+(10e+7)} = 9e+6\,(1, 1, 3, 1, 9e+5, 1, 3, 1, 1, 18e+12),$$

de même on trouve

$$\sqrt{(55e+28)^2+(68e+35)}$$
$$= 55e+28\,(1, 1, 1, 1, 1, 1, 1, 1, 1, 110e+56).$$

14. Les nombres A suivants sont tels que $\sqrt{A}$ aura un développement dont la partie symétrique de la période contiendra dix termes.

A	a	Période										$2a$
61	7	1	4	3	1	2	2	1	3	4	1	14
97	9	1	5	1	1	1	1	1	1	5	1	18
233	15	3	1	3	1	1	1	1	3	1	3	30
298	17	3	1	4	5	1	1	5	4	1	3	34
317	17	1	4	8	1	2	2	1	8	4	1	34
369	19	4	1	3	2	7	7	2	3	1	4	38
554	23	1	1	6	4	1	1	4	6	1	1	46
757	27	1	1	17	1	5	5	1	17	1	1	54
773	27	1	4	13	1	2	2	1	13	4	1	54
794	28	5	1	1	1	1	1	1	1	1	5	56
797	28	4	3	13	1	4	4	1	13	3	4	56

On trouve aussi des formules générales, par exemple

$$\sqrt{(569e+9)^2+(966e+16)} = \sqrt{(231e+4)^2+(520e+9)^2}$$
$$= 569e+9\,(1, 5, 1, 1, 1, 1, 1, 1, 5, 1, 1138e+18),$$

$$\sqrt{(89c+45)^2+(110e+56)} = \sqrt{(80e+41)^2+39e+20)^2}$$
$$= 89e+45\,(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 178e+90).$$

15. Voici les développements dont la partie symétrique de la période contient onze termes. Les six premiers sont donnés dans la table qui suit, les cinq autres s'obtiennent en écrivant dans l'ordre inverse les cinq premiers termes. Pour avoir le développement complet, il convient encore d'ajouter la partie entière a et le dernier terme de la période $2a$.

Exemple $\sqrt{46} = 6\,(1, 3, 1, 1, 2, 6, 2, 1, 1, 3, 1, 12)$.

A	Période						A	Période						A	Période					
46	1	3	1	1	2	6	364	12	1	2	3	1	8	708	1	1	1	1	4	4
76	1	2	1	1	5	4	366	7	1	1	1	2	12	717	1	3	2	12	1	16
103	6	1	2	1	1	9	386	1	1	1	4	1	18	734	10	1	4	1	1	26
127	3	1	2	2	7	11	426	1	1	1	3	2	6	748	2	1	6	5	1	12
184	1	1	3	2	1	2	428	1	2	4	1	5	10	767	1	2	3	1	1	1
213	1	1	2	6	1	8	429	1	2	2	9	1	12	775	1	5	4	1	8	2
236	2	1	3	5	1	6	460	2	4	3	1	2	10	802	3	7	1	3	6	28
239	2	5	1	2	4	15	479	1	7	1	3	2	21	815	1	1	4	1	2	5
247	1	2	1	1	9	1	512	1	1	1	2	6	11	820	1	1	1	2	1	10
263	4	1	1	1	1	15	535	7	1	2	4	1	3	824	1	2	2	1	1	6
276	1	1	1	1	2	2	558	1	1	1	1	1	4	832	1	5	2	2	1	13
295	5	1	2	3	2	6	605	1	1	2	11	1	8	851	5	1	4	2	7	1
304	2	3	2	1	1	1	609	1	2	9	1	1	6	864	2	1	1	5	1	13
329	7	4	2	1	1	4	636	4	1	1	3	3	12	887	1	3	1	1	2	29
351	1	2	1	3	2	2	640	3	2	1	4	1	11	995	1	1	5	4	3	12
355	1	5	3	3	1	6	688	4	2	1	5	7	3							

Voici à titre d'exemple une des formulés générales.

Posons

$$\sqrt{A} = a\,(1,\ 3,\ 1,\ 1,\ 2,\ a,\ 2,\ 1,\ 1,\ 3,\ 1,\ 2a).$$

		3	1	1	2	a	2	1	1	3	1	$\sqrt{A}+a$
$\sqrt{A}-a=$	0	1	3	4	7	18	$18a+7$	$36a+32$	$54a+39$	$90a+71$	$324a+252$	$414a+323$	$(414a+323)(\sqrt{A}+a)+324a+252$
	1	1	4	5	9	23	$23a+9$	$46a+41$	$69a+50$	$115a+91$	$414a+323$	$529a+414$	$(529a+414)(\sqrt{A}+a)+414a+323$

d'où

$$(A - a^2)(529a + 414) = 2a\,(414a + 323) + 324a + 252.$$

Remplaçons a par $23e + 6$, il vient

$$A = (23e + 6)^2 + (36e + 10),$$

$$\sqrt{A} = 23e + 6\,(1, 3, 1, 1, 2, 23e + 6, 2, 1, 1, 3, 1, 46e + 12),$$

cette formule donnne le développement de $\sqrt{A}$ pour $A = 46,\ 887$ quand on y remplace e par 0 ou 1.

16. Voici les valeurs de A qui conduisent à une période dont la partie symétrique contient douze termes.

A	a	Période	$2a$
193	13	1 8 3 2 1 3 3 1 2 3 8 1	26
281	16	1 3 4 1 1 6 6 1 1 4 3 1	32
481	21	1 13 1 1 1 4 4 1 1 1 13 1	42
565	23	1 3 2 1 11 5 5 11 1 2 3 1	46
593	24	2 1 5 2 2 1 1 2 2 5 1 2	48
746	27	3 5 7 1 1 1 1 1 1 7 5 3	54
778	27	1 8 3 5 1 7 7 1 5 3 8 1	54
997	31	1 1 2 1 4 1 1 4 1 2 1 1	62

Bien qu'on ne rencontre pas avec $A \leqslant 1000$ la période constituée par douze termes égaux à l'unité, cette période est possible. Elle s'obtient avec

$$A = (233e + 117)^2 + (288e + 145)$$

$$= (208e + 105)^2 + (105e + 53)^2.$$

Alors $\sqrt{A} = 233e + 117\,(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, (466e + 234).$

17. Développements dont la partie périodique contient treize termes dans la partie symétrique. La table qui suit donne les sept premiers termes. On trouvera la période, en complétant d'abord la partie symétrique par les six termes qu'on trouvera en renversant l'ordre des six premiers termes et en écrivant le dernier terme $2a$, a étant la partie entière.

Exemple $\sqrt{134} = 11\ (1, 1, 2, 1, 3, 1, 10, 1, 3, 1, 2, 1, 1, 22)$.

A	Période							A	Période							A	Période						
134	1	1	2	1	3	1	10	422	1	1	5	2	1	3	20	692	3	3	1	2	1	1	12
179	2	1	1	1	3	5	13	430	1	2	1	3	1	6	8	699	2	3	1	1	2	1	25
190	1	3	1	1	1	2	2	467	1	1	1	1	3	3	21	713	1	2	2	1	4	6	2
201	5	1	1	1	2	1	8	471	1	2	2	1	3	4	14	722	1	6	1	2	3	2	26
212	1	1	3	1	1	1	6	472	1	2	1	1	1	4	5	737	6	1	3	3	7	2	4
251	1	5	2	1	2	2	15	474	1	3	2	1	1	1	6	742	4	5	1	4	8	1	6
262	5	2	1	2	1	10	16	500	2	1	3	2	1	1	10	745	3	2	1	1	5	2	10
307	1	1	11	5	1	3	17	502	2	2	7	14	1	4	22	806	2	1	1	3	2	5	4
319	1	6	5	1	4	3	1	548	2	2	3	1	5	1	10	807	2	2	4	1	3	4	9
340	2	3	1	1	1	1	8	561	1	2	5	1	1	2	2	825	1	2	1	1	1	1	4
341	2	6	1	8	2	1	2	587	4	2	1	1	1	1	23	833	1	6	4	3	2	1	2
347	1	1	1	2	4	1	17	611	1	2	1	1	4	2	1	838	1	18	3	6	9	2	28
356	1	6	1	1	2	1	8	667	1	4	1	3	7	8	2	916	3	1	3	3	1	1	14
388	1	2	3	4	12	1	8	670	1	7	1	1	1	5	10	934	1	1	3	1	1	3	30
406	6	1	2	4	7	1	4	683	7	2	4	3	1	1	25	954	1	7	1	5	3	2	6

Chacun de ces développements peut conduire à une formule générale contenant k ($k = 1$ à 8) paramètres.

Ainsi on trouve

$$\sqrt{(377e + 189)^2 + (466e + 234)}$$
$$= 337e + 189\,(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 754e + 378),$$

si on exige que la période soit constituée par treize termes égaux à 1.

18. Voici les développements dont la partie périodique contient quatorze termes.

A	a	Période													
109	10	2	3	1	2	4	1	6	6	1	4	2	1	3	2	20
353	18	1	3	1	2	1	1	1	1	1	1	2	1	3	1	36
449	21	5	3	1	1	7	1	5	5	1	7	1	1	3	5	42
461	21	2	8	10	1	1	1	1	1	1	1	1	10	8	2	42
617	24	1	5	4	2	1	6	2	2	6	1	2	4	5	1	48
685	26	5	1	3	1	12	3	2	2	3	12	1	3	1	5	52
709	26	1	1	1	2	7	4	3	3	4	7	2	1	1	1	52
877	29	1	1	1	1	2	4	1	1	4	2	1	1	1	1	58

Chacun de ces développements peut conduire à une formule générale contenant un, deux, trois, quatre, cinq, six, sept ou huit paramètres.

19. On trouvera de même les développements suivants dont la partie périodique contient quinze termes dans la partie symétrique.

Comme précédemment, nous ne donnons que les huit premiers termes, le dernier étant celui du milieu de la partie symétrique.

A	Période	A	Période	A	Période
94	1 2 3 1 1 5 1 8	385	1 1 1 1 1 3 1 2	679	17 2 1 5 8 1 1 25
124	7 2 1 1 1 3 1 4	391	1 3 2 2 1 1 2 19	686	5 4 1 1 3 2 10 26
133	1 1 7 5 1 1 1 2	415	2 1 4 4 6 1 1 3	750	2 1 1 2 3 1 1 8
172	8 1 2 2 1 1 3 6	431	1 3 5 1 2 7 1 19	846	11 1 1 1 1 1 1 2
191	1 4 1 1 3 2 2 13	446	8 2 2 1 3 1 1 20	861	2 1 11 14 1 1 2 2
217	1 2 1 2 1 1 9 4	496	3 1 2 4 1 1 2 2	875	1 1 2 1 1 1 1 3
249	1 3 1 1 5 1 3 10	513	1 1 1 5 1 4 5 2	878	1 1 1 2 2 4 1 28
261	6 2 3 7 1 3 1 2	542	3 1 1 3 1 1 1 22	917	3 1 1 4 1 14 3 8
284	1 5 1 3 2 1 4 8	550	2 4 1 2 1 1 7 4	928	2 6 3 1 1 1 8 15
302	2 1 1 1 4 2 1 16	639	3 1 1 2 4 4 1 4	944	1 2 1 1 1 2 2 3
310	1 1 1 1 5 3 1 2	647	2 3 2 2 1 1 4 25	950	1 4 1 1 1 1 1 2
311	1 1 1 2 1 6 3 17	654	1 1 2 1 9 1 1 16	955	1 9 3 6 1 1 5 12
343	1 1 11 1 5 3 1 17	655	1 1 2 5 3 2 8 10	969	7 1 3 3 1 1 1 2
376	2 1 1 3 1 2 2 4	666	1 4 5 1 1 6 1 4	988	2 3 4 1 20 6 1 14

On trouve des formules contenant k ($k = 1$ à 9) paramètres.

Par exemple

$$\sqrt{(987e + 494)^2 + (1220e + 611)}$$
$$= 987e + 494\,(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1974e + 988).$$

20. Voici les développements conduisant à une période de seize termes.

A	a	Période
157	12	1 1 7 1 5 2 1 1 1 1 2 5 1 7 1 1 24
241	15	1 1 9 1 5 3 3 1 1 3 3 5 1 9 1 1 30
313	17	1 2 4 11 1 1 3 2 2 3 1 1 11 4 2 1 34
829	28	1 3 1 4 2 3 2 1 1 2 3 2 4 1 3 1 56
857	29	3 1 1 1 3 1 6 1 1 6 1 3 1 1 1 3 58
941	30	1 2 11 1 14 2 2 1 1 2 2 14 1 11 2 1 60

On trouve par exemple

$$\sqrt{(1597e + 799)^2 + (1974e + 988)} = \sqrt{(715e + 358)^2 + (1428e + 715)^2}$$
$$= 1597e + 799\,(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 3194e + 1598).$$

21. Nous donnons ci-dessous tous les développements de $\sqrt{A}$ ($A \leqq 1000$) quand la période contient plus de seize termes dans la partie symétrique. Nous donnons chaque fois $\frac{n+1}{2}$ terme si le nombre n de termes est impair. Dans ce cas le dernier terme est celui du milieu de la partie symétrique.

Si le nombre n de termes est pair, on fera figurer $\frac{n}{2}$ termes. Dans tous les cas, on achèvera la période par la deuxième moitié et la complètera par le terme $2a$, a étant la partie entière.

A	Période	A	Période
	1° Dix-sept termes dans la partie symétrique.		
139	1 3 1 3 7 1 1 2 11	758	1 1 7 2 1 3 3 1 26
163	1 3 3 2 1 1 7 1 11	781	1 17 1 1 1 5 1 1 4
283	1 4 1 1 1 3 10 1 15	787	18 1 2 5 1 8 1 1 27
417	2 2 1 1 1 5 4 1 12	805	2 1 2 5 1 13 2 1 10
419	2 7 1 2 3 1 2 1 19	831	1 4 1 3 1 1 1 1 18
424	1 1 2 4 5 1 1 1 9	873	1 1 4 1 6 1 1 3 6
519	1 3 1 1 2 1 2 3 7	879	1 1 1 5 3 1 3 2 9
549	2 3 9 11 1 1 1 1 4	951	1 5 5 2 3 1 1 1 9
562	1 2 2 2 4 1 5 1 22	976	4 6 1 2 3 1 4 2 3
566	1 3 1 3 1 1 8 1 22	998	1 1 2 4 8 1 3 1 30
633	6 3 1 2 2 1 1 2 16	1000	1 1 1 1 1 6 2 2 15
	2° Dix-huit termes		
337	2 1 3 1 11 2 4 1 3	865	2 2 3 3 1 1 1 2 6
509	1 1 3 1 1 2 10 1 8	922	2 1 2 1 9 2 1 1 6
521	1 4 1 2 1 2 8 1 3	929	2 11 1 2 3 2 7 5 2
569	1 5 1 5 9 2 1 2 3	977	3 1 8 5 1 1 3 7 1
653	1 1 4 7 12 1 1 1 3		
	3° Dix-neuf termes		
151	3 2 7 1 3 4 1 1 1 11	537	5 1 3 2 1 1 1 2 1 14
199	9 2 1 2 2 5 4 1 1 13	559	1 1 1 4 15 1 1 4 1 2
268	2 1 2 3 3 1 3 1 10 8	606	1 1 1 1 1 1 2 1 9 8
367	6 2 1 3 1 1 2 1 12 19	622	1 15 1 1 1 4 1 7 2 24
393	1 4 1 2 4 1 1 1 1 12	790	9 2 1 5 1 1 3 4 1 4
409	4 2 7 1 1 1 4 2 2 13	801	3 3 4 1 5 2 10 1 6 6
412	3 2 1 3 1 4 3 2 13 10	863	2 1 1 1 7 1 3 3 5 29
477	1 5 3 1 4 10 1 2 2 4	972	5 1 1 1 7 6 1 3 1 14
511	1 1 1 1 6 1 14 4 1 21	996	1 1 3 1 2 2 1 1 1 4
524	1 8 5 1 1 1 1 2 1 10	999	1 1 1 1 5 6 1 5 1 5

A	Période	A	Période

4° Vingt termes

181	2	4	1	8	6	1	1	1	1	2	433	1	4	4	2	2	1	3	13	1	1
277	1	1	1	4	10	1	7	2	2	3	641	3	6	1	9	3	1	3	1	5	1
394	1	5	1	1	1	3	1	3	5	2	809	2	3	1	7	2	1	6	2	3	11
397	1	12	3	4	9	1	2	1	2	1	953	1	6	1	2	1	3	8	1	1	4

5° Vingt-et-un termes

166	1	7	1	1	1	2	4	1	3	2	12	662	1	2	1	2	3	1	1	2	6	1	24
253	1	9	1	1	1	2	1	7	4	2	2	664	1	3	3	5	2	2	1	1	2	1	5
466	1	1	2	2	1	2	5	1	3	1	20	763	1	1	1	1	1	5	1	1	17	1	6
489	8	1	4	1	1	1	3	2	1	2	14	771	1	3	3	2	4	1	1	1	1	2	27
491	6	3	4	8	1	1	1	2	1	1	21	834	1	7	3	1	2	1	1	1	3	2	28
517	1	2	1	4	3	3	2	10	1	14	4	893	1	7	1	1	4	14	1	2	1	1	2
523	1	6	1	1	1	4	2	3	14	1	21	931	1	1	19	1	5	6	1	1	1	1	2
596	2	2	2	1	1	1	6	2	1	9	12	932	1	1	8	4	1	1	2	1	1	1	14
597	2	3	3	1	3	1	2	11	1	6	16	947	1	3	2	2	2	1	4	1	7	1	29
637	5	4	2	1	3	1	1	12	16	1	2	971	6	4	1	1	1	2	5	3	2	12	31
643	2	1	3	1	16	8	2	1	1	5	25												

6° Vingt-deux termes

586	4	1	4	1	1	2	1	2	7	1	2	853	4	1	5	1	2	4	1	1	14	19	2
634	5	1	1	2	1	4	3	6	1	7	1												

7° Vingt-trois termes

271	2	6	10	1	4	1	1	2	1	2	1	15	753	2	3	1	2	1	1	1	7	4	1	6	18
382	1	1	5	12	1	5	1	1	2	3	1	18	789	11	4	1	1	2	3	1	13	3	1	2	18
581	9	1	1	1	1	1	3	11	1	3	2	6	826	1	2	1	5	1	1	1	3	5	2	9	8
607	1	1	1	3	7	1	15	1	1	4	1	23	871	1	1	19	5	1	5	1	2	1	1	1	1
681	10	2	2	1	1	2	6	7	3	2	1	16	911	5	2	8	5	1	11	4	4	2	1	1	29

8° Vingt-quatre termes

457	2	1	1	1	5	2	13	1	3	1	4	1	881	1	2	7	11	1	2	1	3	1	4	1	1

9° Vingt-cinq termes

211	1	1	9	5	1	2	2	1	1	4	3	1	13	553	1	1	15	5	1	4	2	1	1	3	1	2	6
214	1	1	1	2	3	1	4	9	1	1	5	3	14	614	1	3	1	1	9	2	1	4	3	1	1	2	24
244	1	1	1	1	1	2	1	5	1	1	9	1	6	628	16	1	2	5	4	2	1	2	2	3	1	3	12
301	2	1	6	3	1	2	2	1	1	8	11	2	4	657	1	1	1	6	1	1	1	2	1	1	5	1	4
309	1	1	2	1	2	4	1	1	1	8	6	1	10	749	2	1	2	1	1	4	2	1	1	13	10	1	6
331	5	5	1	1	2	1	2	1	11	2	1	1	17	835	1	8	1	1	1	5	1	3	3	1	1	2	5
358	1	11	1	1	1	3	1	1	4	1	5	2	18	856	3	1	7	1	1	1	1	4	3	1	2	6	7
547	2	1	1	2	1	2	1	7	15	2	6	5	23														

10° Si n est le nombre de termes de la partie symétrique de la période, on trouve

949	1 4 6 1 1 1 4 2 14 1 19 1 1	$n=26$
334	3 1 1 1 2 5 1 2 2 11 1 3 7 18	$n=27$
487	14 1 2 4 1 1 3 2 5 1 6 1 1 21	
501	2 1 1 1 1 3 8 1 2 10 1 5 2 14	
599	2 9 3 2 1 1 3 1 6 4 1 2 1 23	
716	1 3 7 2 1 1 6 10 1 1 4 2 1 12	
719	1 4 2 1 1 1 1 1 4 3 1 9 1 25	
869	2 11 3 2 1 1 1 1 1 14 8 2 1 4	
926	2 3 11 1 7 1 3 2 5 1 1 1 4 30	
821	1 1 1 7 1 1 10 1 13 2 2 2 1 1	$n=28$
379	2 7 3 2 2 6 12 1 4 1 1 1 3 4 19	$n=29$
436	1 7 2 1 1 1 13 3 2 2 5 1 1 4 10	
772	1 3 1 1 1 5 1 1 7 2 1 1 17 1 12	
849	7 3 1 2 1 7 1 1 2 4 11 2 2 1 18	
946	1 3 8 1 1 6 3 3 1 3 1 1 1 2 30	
981	3 8 1 1 1 1 1 1 2 1 1 15 12 2 6	
601	1 1 15 1 5 5 3 1 1 2 1 2 2 1 9	$n=30$
673	1 16 3 5 2 3 1 1 6 1 5 1 1 1 1	
463	1 1 13 1 5 4 1 1 1 1 2 2 6 1 3 21	$n=31$
508	1 1 5 1 14 5 1 1 3 4 1 2 1 1 1 10	
764	1 1 1 3 1 1 2 2 1 6 4 1 7 10 1 12	
913	4 1 1 1 2 1 1 6 7 2 2 19 1 2 1 4	
956	1 11 2 1 1 1 1 7 8 1 2 2 1 2 1 14	
967	10 2 1 6 4 3 2 2 1 1 8 3 2 1 20 31	
974	4 1 3 1 1 1 11 1 5 3 8 1 1 1 1 30	
989	2 4 2 1 11 1 8 15 1 1 1 1 2 1 2 2	
613	1 3 6 1 4 1 1 1 3 2 11 1 15 1 1 2	$n=32$
937	1 1 1 1 3 4 2 3 6 1 1 19 1 6 1 2	
454	3 3 1 13 2 3 2 1 1 4 6 1 7 1 1 1 20	$n=33$
921	2 1 6 1 11 3 1 2 2 3 1 1 1 1 1 8 20	
958	1 19 1 1 1 6 4 1 1 1 1 2 1 4 1 9 2	
964	20 1 2 6 1 1 3 1 1 1 1 11 1 4 3 1 14	
478	1 6 3 4 1 1 5 1 2 3 1 1 1 1 1 13 1 20	$n=35$
546	1 1 2 1 1 1 3 3 2 1 5 5 15 1 1 8 1 10	
652	1 1 6 1 3 1 3 2 5 1 16 5 1 1 1 1 2 12	
421	1 1 13 5 1 3 1 2 1 1 1 2 9 1 7 3 3 2	$n=36$
769	1 2 1 2 1 1 17 1 10 6 1 5 3 3 2 1 1 1	
526	1 14 3 4 1 3 2 1 3 1 8 2 1 1 2 6 7 2 22	$n=37$
619	1 7 3 5 4 1 3 1 2 1 1 9 2 1 1 1 15 1 23	
669	1 6 2 2 3 1 9 1 1 2 1 12 4 1 1 1 1 1 16	
691	3 2 17 10 2 5 2 1 2 1 4 1 1 8 4 1 1 1 25	
811	2 10 1 8 1 1 2 1 1 1 3 6 18 1 4 1 2 1 27	

541	3 1 5 1 8 2 4 1 2 3 1 1 11 15 2 2 1 1 1	$n=38$
661	1 2 2 4 4 16 1 9 2 1 12 5 1 1 1 2 1 3 1	
589	3 1 2 2 15 1 3 9 2 4 1 11 3 6 1 1 1 1 3 2	$n=39$
604	1 1 2 1 3 2 1 1 1 4 1 5 3 9 1 1 15 1 6 12	
718	1 3 1 8 7 1 1 5 2 2 1 2 3 1 3 17 1 1 2 26	
721	1 5 1 2 1 2 1 1 1 1 1 1 17 3 1 1 10 5 1 6	
862	2 1 3 1 1 9 4 2 2 2 1 5 1 4 2 19 8 2 1 28	
571	1 8 1 1 2 1 1 1 15 3 2 1 6 7 1 4 2 3 4 2 23	$n=41$
724	1 9 1 3 1 1 2 1 4 5 1 3 3 3 17 1 1 1 2 1 12	
889	1 4 2 3 1 1 11 2 1 3 19 1 1 1 1 6 1 5 1 3 8	
907	8 1 1 2 2 1 19 2 1 2 5 9 1 5 1 3 1 3 1 1 29	
766	1 2 10 1 2 1 3 1 1 17 1 8 3 1 1 2 1 2 5 5 1 26	$n=43$
796	4 1 2 5 1 10 2 3 1 6 3 1 1 1 1 2 4 1 2 1 18 14	
823	1 2 4 1 7 2 1 1 1 1 8 1 18 4 2 1 3 2 2 5 1 27	
694	2 1 9 1 6 1 1 1 1 1 2 1 8 17 2 4 3 3 2 4 1 5 26	$n=45$
739	5 2 2 1 1 3 3 2 1 8 2 1 2 1 17 2 1 1 7 5 1 10 27	
844	19 2 1 5 1 3 1 1 1 1 2 6 1 7 2 3 2 2 11 4 1 3 14	
859	3 4 5 1 1 1 2 2 3 2 19 9 1 2 1 1 4 1 3 11 2 6 29	
883	1 2 1 1 19 4 5 6 2 2 2 1 2 1 1 2 8 9 1 3 1 2 29	
631	8 2 1 4 1 9 4 2 6 1 2 1 2 1 1 1 1 4 2 2 2 1 16 25	$n=47$
751	2 2 8 1 2 1 3 5 1 4 1 1 1 3 1 1 3 10 1 2 7 2 17 1 4 27	$n=51$
886	1 3 3 1 2 1 1 5 2 1 1 1 9 3 2 1 1 19 3 1 11 6 1 1 7 1 28	$n=53$
991	2 12 10 2 2 2 1 1 2 6 1 1 1 1 3 1 8 4 1 2 1 2 3 1 4 1 20 6 4 31	$n=59$
919	3 5 1 2 1 2 1 1 1 2 3 1 1 19 2 3 1 1 4 9 1 7 1 3 6 2 11 1 1 1 29	$n=61$

22. Certaines combinaisons ne se rencontrent jamais dans la partie symétrique de la période. Ainsi il n'arrive jamais que la partie symétrique de la période soit constituée de deux termes égaux impairs. Il en est de même, si la partie symétrique de la période est constituèe de $3a + 2$ termes égaux à l'unité.

Mais, par contre, certaines combinaisons sont toujours possibles. Nous allons en examiner quelques-unes.

Théorème.— Toute combinaison possible de la partie symétrique de la période se rencontre une infinité de fois.

Soit un développement $\sqrt{A} = a\,(S, 2a)$ dans lequel on a écrit S pour l'ensemble de termes formant la partie symétrique de la période.

Si on pose

$$x = y\,(\mathrm{S},\, 2y),$$

on sera conduit à une équation de la forme

$$x - y = \frac{\mathrm{P}\,(x + y) + \mathrm{R}}{\mathrm{Q}\,(x + y) + \mathrm{P}},$$

$\frac{\mathrm{P}}{\mathrm{Q}}$ étant la réduite qu'on obtient en arrêtant le développement après la partie symétrique, et $\frac{\mathrm{R}}{\mathrm{P}}$ la réduite précédente.

On en tire

$$\mathrm{Q}\,(x^2 - y^2) = 2\mathrm{P}y + \mathrm{R}.$$

Cette équation sera possible, car elle admet la solution

$$y = a, \qquad x = \mathrm{A}.$$

On pourra poser par exemple

$$y = a + \mathrm{Q}e,$$

et à chaque valeur entière de e correspond une valeur entière de y donnant une valeur entière de x.

23. Théorème. — Tout développement dont la partie symétrique est constituée par des termes égaux pairs est possible, quel que soit ce nombre de termes.

Soit le développement dont la partie symétrique est constituée par q terme $2k$, dont l'ensemble sera désigné par S.

Considérons le développement

$$\sqrt{k^2 + 1} = k\,(2k),$$

que nous pouvons écrire

$$\sqrt{k^2 + 1} = k\,(2k,\, 2k,\, 2k,\, \ldots,\, 2k), \qquad (q + 1 \text{ fois } 2k),$$

ou

$$\sqrt{k^2 + 1} = k\,(\mathrm{S},\, 2k).$$

Posons

$$x = y\,(\mathrm{S},\, 2y),$$

cette équation est possible et admet une infinité de solutions d'après le paragraphe précédent. On aura ainsi une infinité de développements dont la partie symétrique sera S — c'est-à-dire, constituée de q termes égaux à $2k$.

Applications. — 1° Soit à chercher les valeurs de A pour lesquelles la période sera constituée dans la partie symétrique de n termes égaux chacun à 2.

Soit la suite

$$u_1 = 1, \quad u_2 = 2, \quad u_{i+2} = 2u_{i+1} + u_i,$$

et posons

$$\sqrt{A} = a\,(2, 2, \overset{n \text{ fois}}{\ldots\ldots}, 2, 2a),$$

$$\sqrt{A} - a = \frac{u_n(\sqrt{A} + a) + u_{n-1}}{u_{n+1}(\sqrt{A} + a) + u_n},$$

ou

$$(A - a^2)\,u_{n+1} = 2u_n a + u_{n-1}.$$

Cela étant, considérons d'abord le cas quand n est pair, alors u_n est pair.

Posons

$$n = 2k, \quad a = u_{2k+1}e + 1,$$

il vient

$$A = a^2 + 1 + 2u_{2k}e = (u_{2k+1}e + 1)^2 + (2u_{2k}e + 1).$$

Si n est impair, l'équation précédente se simplifie par 2 et il vient, u_n étant impair et $u_{n\pm1}$ pair

$$2a = u_{n+1}e + 2, \quad A = a^2 + (u_n e + 1).$$

On trouve ainsi

$n = 0$,	$A = e^2 + 1$,	$\sqrt{A} = e\,(2e)$,
1,	$e^2 + e$,	$e\,(2, 2e)$,
2,	$(5e + 1)^2 + (4e + 1)$,	
ou	$(3e + 1)^2 + (4e + 1)^2$,	$5e + 1\,(2, 2, 10 + 2)$,
3,	$(6e + 1)^2 + (5e + 1)$,	$6e + 1\,(2, 2, 2, 12 + 2)$,
4,	$(29e + 1)^2 + (24e + 1)$,	
ou	$(21e + 1)^2 + (20e + 1)^2$,	$29e + 1\,(2, 2, 2, 2, 58e + 2)$,
5,	$(35e + 1)^2 + (29e + 1)$,	$35e + 1\,(2, 2, 2, 2, 2, 70e + 2)$,
6,	$(169e + 1)^2 + (140e + 1)$,	
	$= (119e + 1)^2 + (120e + 1)^2$,	$169e + 1\,(2, 2, 2, 2, 2, 2, 338e + 2)$,

2° Cherchons un développement dont la partie symétrique de la période est constituée par n termes égaux chacun à 4.

Considérons la suite

$$u_1 = 1, \qquad u_2 = 4, \qquad u_{i+1} = 4u_i + u_{i-1},$$

et posons

$$\alpha = \sqrt{A} = a\,(4,\ 4,\ \overset{n \text{ fois}}{\ldots},\ 4,\ 2a),$$

$$\alpha - a = \frac{u_n(\alpha + a) + u_{n-1}}{u_{n+1}(\alpha + a) + u_n},$$

ou

$$u_{n+1}(\alpha^2 - a^2) = 2u_n a + u_{n-1}.$$

Si n est pair on aura, u_{n+1} étant impair,

$$a = u_{n+1}e + 2, \qquad A = \alpha^2 = (u_{n+1}e + 2)^2 + (2u_n e + 1).$$

Si n est impair, l'équation se simplifie par 2 et on aura

$$2a = u_{n+1}e + 4, \qquad A = \alpha^2 = \left(\frac{u_{n+1}}{2}e + 2\right)^2 + \left(u_n e + 1\right).$$

On trouve ainsi

$n = 0$,	$\alpha^2 = e^2 + 1$,	$\alpha = e\,(2e)$.
1,	$4e^2 + e$,	$2e\,(4,\ 4e)$.
2,	$(17e + 2)^2 + (8e + 1)$,	
ou	$(15e + 2)^2 + (8e + 1)^2$,	$17e + 2\,(4,\ 4,\ 34e + 4)$,
3,	$(36e + 2)^2 + (17e + 1)^2$,	$36e + 2\,(4,\ 4,\ 4,\ 72e + 4)$,
4,	$(305e + 2)^2 + (144e + 1)$,	
ou	$((273e + 2)^2 + (136e + 1)^2$,	$305e + 2\,(4,\ 4,\ 4,\ 4,\ 610e + 4)$.

24. Théorème.— Il existe une infinité de développements dont la période (ou la partie symétrique de la période) est constituée par un nombre donné de termes.

En effet, il suffit de prendre tous ces termes égaux à un nombre pair donné et le développement sera possible.

CHAPITRE IV.

Développement en fraction continue de la racine positive de l'équation $x^2 + x - A = 0$.

1. Considérons le nombre algébrique de second degré α

$$\alpha = \frac{-1 + \sqrt{1 + 4A}}{2},$$

racine positive de l'équation

$$x^2 + x - A = 0,$$

et développons α en fraction continue. On aura

$$\alpha = a, x_1, x_2, \ldots, x_k, \ldots.$$

Ce développement est infini et indéfiniment périodique. La période commence au deuxième quotient incomplet et comprend $k + 1$ termes dont le dernier est $2a + 1$, les k autres termes forment une suite symétrique.

On aura ainsi

$$\alpha = a\,(x_1, x_2, x_3, \ldots, x_k, 2a + 1),$$

avec les relations

$$x_i = x_{k-i+1}. \qquad \text{(p. 18).}$$

On suppose que $1 + 4A$ n'est pas un carré parfait, car autrement α serait rationnel. Ainsi A ne peut pas être le double d'un triangulaire, car si $A = n^2 + n$, on aura

$$1 + 4A = (2n + 1)^2, \qquad \text{et} \qquad \alpha = n.$$

Ainsi on ne considérera point cette équation pour

A = 0, 2, 6, 12, 20, 30, 42, 56, 72, 90, 110, 132, 156, 182, 210, 240, 272, 306, 342, 380, 420, 462, 506, 552, 600, 650, 702, 756, 812, 870, 930, 992, etc.

2. *Inversement, si le développement de* α *est tel que nous avons vu au numéro précédent, la quantité* α *est racine de* $\alpha^2 + \alpha - A = 0$.

Soit

$$\alpha = a\,(x_1, x_2, x_3, \ldots, x_k\,,\, 2a + 1),$$

ou

$$\alpha - a = 0, x_1, x_2, x_3, \ldots, x_k\,,\, \alpha + a + 1.$$

Soit encore

$$\frac{P}{Q} = 0, x_1, x_2, x_3, \ldots, x_k,$$

et soit $\frac{R}{P}$ [1] la réduite qui précède $\frac{P}{Q}$ c'est-à-dire

$$\frac{R}{P} = 0, x_1, x_2, x_3, \ldots, x_{k-1}.$$

On aura

$$\alpha - a = \frac{P\,(\alpha + a + 1) + R}{Q\,(\alpha + a + 1) + P},$$

ou

$$Q\,(\alpha^2 - a^2) + Q\alpha = Qa + 2Pa + P + R.$$

Cette équation est de la forme

$$\alpha^2 + \alpha - A = 0.$$

Avec

$$A = a^2 + a + \frac{2Pa + P + R}{Q}.$$

3. On peut avoir $k = 0$. La période sera constituée par le seul terme irrégulier et on aura

$$\sqrt{A} = a\,(2a + 1),$$

ou bien

$$\alpha^2 + \alpha - (a^2 + a + 1) = 0, \qquad (1)$$

d'où

$$A = a^2 + a + 1.$$

On aura ainsi le développement de la racine de l'équation

$$\alpha^2 + \alpha - A = 0,$$

---

(1) Voir note au bas de la page 30.

avec

A = 1, 3, 7, 13, 21, 31, 43, 57, 73, 91, 111, 133, 157, 183, 211, 241, 273, 307, 343, 381, 421, 463, 507, 553, 601, 651, 703, 757, 813, 871, 931, 993, etc.

4. Il peut arriver que la période soit constituée d'un seul terme dans la partie symétrique.

Soit

$$\alpha = a\,(x,\ 2a+1),$$

un tel développement, on trouve

$$\alpha - a = 0,\ x,\ \alpha + a + 1,$$

ce qui conduit à l'équation

$$x^2\,(\alpha^2 - a^2) + x\,(\alpha - a) - (2a+1) = 0.$$

On est ainsi conduit à poser

$$\left.\begin{array}{c} 2a+1 = xe. \\ \text{Alors} \\ A = a^2 + a + e, \\ \text{donne} \\ \alpha^2 + \alpha - A = 0, \\ \text{et} \\ \alpha = a\,(x,\ 2a+1). \end{array}\right\} \quad (2)$$

On trouve ainsi le développement de la racine de l'équation

$$\alpha^2 + \alpha - A = 0,$$

pour

A = 5, 11, 19, 23, 29, 41, 55, 59, 61, 71, 89, 109, 113, 117, 131, 155, 161, 181, 185, 191, 209, 239, 271, 275, 283, 305, 311, 313, 341, 379, 383, 393, 419, 461, 505, 509, 511, 515, 521, 551, 599, 607, 649, 653, 657, 701, 755, 761, 767, 811, 815, 831, 869, 929, 991, 999, etc.

On peut trouver des formules moins générales en précisant la valeur de x ou celle de a.

Ainsi $x = 1$ donne

$$e = 2a+1, \qquad A = a^2 + 3a + 1, \qquad \alpha = a\,(1,\ 2a+1).$$

Si on fait $a = 3k + 1$, on trouve $2a + 1 = 6k + 3$, alors

$$\begin{array}{lll} x = 1 \text{ donne } & e = 6k + 3, \text{ alors } & A = 9k^2 + 15k + 5, \\ \quad 3 & \quad 2k + 1, & \quad 9k^2 + 11k + 3, \\ \quad 2k + 1 & \quad 3 & \quad 9k^2 + 9k + 5. \end{array}$$

5. Il peut arriver que la période soit constituée par deux termes dans la partie symétrique.

Soit

$$\alpha = a\,(x, x, 2a + 1),$$

un tel développement, on trouve

$$\alpha - a = 0, x, x, \alpha + a + 1 = \frac{0 \,\Big|\, 1 \,\Big|\, x \,\Big|\, x\,(\alpha + a + 1) + 1}{1 \,\Big|\, x \,\Big|\, x^2 + 1 \,\Big|\, (x^2 + 1)(\alpha + a + 1) + x}$$

d'où

$$(\alpha - a)(x^2 + 1)(\alpha + a + 1) + x\,(\alpha - a) - x\,(\alpha + a + 1) - 1 = 0,$$

ou bien

$$(\alpha^2 - a^2)(x^2 + 1) + (\alpha - a)(x^2 + 1) - (2ax + x + 1) = 0.$$

On trouve en posant

$$\left.\begin{array}{l} 2ax + x + 1 = (x^2 + 1)\,e, \\ A = a^2 + a + e, \\ \alpha = a\,(x, x, 2a + 1). \end{array}\right\} \quad (3)$$

On peut trouver un grand nombre de formules moins générales en précisant la valeur de x. Nous donnons ci-dessous quelques-unes de ces formules.

1° $x = 1$ donne

$$e = a + 1, \qquad A = (a + 1)^2 = e^2, \qquad \alpha = a\,(1, 1, 2a + 1).$$

On aura ainsi le développement de α pour

A = 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, 256, 289, 324, 361, 400, 441, 484, 529, 576, 625, 676, 729, 784, 841, 900, 961, etc.

2° Si on fait $x = 2$, on trouve

$$a = 5k + 3, \qquad e = 4k + 3, \qquad A = 25k^2 + 39k + 15.$$

On aura ainsi le développement de α pour

$$A = 15, 79, 193, 357, 571, 835, \text{etc.}$$

3° $x = 3$ donne

$$A = 25k^2 + 18k + 3, \qquad \alpha = 5k + 1\ (3, 3, 10k + 3).$$

Ceci donnera le développement de α pour

$$A = 46, 139, 282, 475, 718, \text{etc.}$$

4° $x = 4$ donne $A = 289k^2 + 365k + 115$, d'où $A = 115, 769$, etc.,

$x = 5$	$169k^2 + 70k + 7$,		246, 795,
$x = 6$	$a = 37k + 21$,	$e = 12k + 7$,	469,
$x = 7$	$25k + 3$.	$7k + 1$,	820,
$x = 8$	$65k + 36$,	$16k + 9$,	
$x = 9$	$41k + 4$.	$9k + 1$, etc.	

5. On peut avoir trois termes dans la partie symétrique du développement de α.

Soit

$$\alpha = a\ (x, y, x, 2a + 1)$$

un tel développement, on aura

$$\alpha - a = 0, x, y, x, \alpha + a + 1$$

$$= \begin{array}{c|c|c|c|c}
 & & y & x & \alpha + a + 1 \\
\hline
0 & 1 & y & xy + 1 & (xy + 1)(\alpha + a + 1) + y \\
\hline
1 & x & xy + 1 & x^2y + 2x & (x^2y + 2x)(\alpha + a + 1) + xy + 1
\end{array}$$

On trouvera comme dans le cas du développement de $\sqrt{A}$ des formules générales conduisant à tout développement donné d'avance, pourvu que ce développement soit possible.

Il est plus aisé de se donner un développement possible et de chercher les valeurs de A qui y conduisent.

Ainsi $\alpha^2 + \alpha - 8 = 0$ conduit à $\alpha = 2\,(2, 1, 2, 5)$.

Posons

$$\alpha = a\,(2, 1, 2, 2a + 1),$$

d'où

$$8\,(\alpha^2 - a^2) + 8\alpha - (14a + 4) = 0. \qquad (4)$$

Si dans cette équation on fait $a = 4e + 2$, on trouve

$$14a + 4 = 56e + 32 = 8\,(7e + 4),$$

et (4) devient

$$\alpha^2 + \alpha - (a^2 + 7e + 2) = 0,$$

Ainsi

$$A = a^2 + 7e + 2 = (4e + 2)^2 + (7e + 4).$$

On aura ainsi non seulement le développement de α pour $A = 8$, ce qu'on obtient avec $e = 0$, mais encore le développement de α pour

$$A = 47, 118, 221, 356, 523, 722, 953, \text{etc.}$$

Voici quelques formules générales donnant lieu pour le développement de α à des périodes composées de trois termes dans la partie symétrique

$$A = (7e + 2)^2 + (19e + 7), \qquad \alpha = 7e + 2\,(1, 5, 1, 14e + 5).$$

On trouvera α pour $A = 107, 301, 593, 983$.

$$A = (9e + 3)^2 + (25e + 10), \qquad \alpha = 9e + 3\,(1, 7, 1, 18e + 7),$$
$$A = 179, 501, 985,$$

$$A = (11e + 4)^2 + (31e + 13), \qquad \alpha = 11e + 4\,(1, 9, 1, 22e + 9),$$
$$A = 269, 751,$$

$$A = (13e + 5)^2 + (37e + 16), \qquad \alpha = 13e + 5\,(1, 11, 1, 26e + 11),$$
$$A = 377,$$

$$A = (15e + 6)^2 + (43e + 19), \qquad \alpha = 15e + 6\,(1, 13, 1, 30e + 13),$$
$$A = 503,$$

$$A = (17e + 7)^2 + (49e + 22), \qquad \alpha = 17e + 7\,(1, 15, 1, 34e + 15),$$
$$A = 647,$$

$$A = (19e + 8)^2 + (55e + 25), \qquad \alpha = 19e + 8\,(1, 17, 1, 38e + 17),$$
$$A = 809,$$

$$A = (21e + 9)^2 + (61e + 28), \qquad \alpha = 21e + 9\,(1, 19, 1, 42e + 19),$$
$$A = 989.$$

On trouve de même

$A = (3e + 1)^2 + e,$ $\alpha = 3e\,(1, 1, 1, 6e + 1),$

$A = (4e + 2)^2 + (7e + 4)$ $\alpha = 4e + 2\,(2, 1, 2, 8e + 5),$

$A = (15e + 5)^2 + (23e + 8),$ $\alpha = 15e + 5\,(3, 1, 3, 30e + 11),$

$A = (12e + 9)^2 + (17e + 13),$ $\alpha = 12e + 9\,(4, 1, 4, 24e + 19),$

$A = 94, 471, 947,$

$A = (35e + 14)^2 + (47e + 19),$ $\alpha = 35e + 14\,(5, 1, 5, 70e + 29),$

$A = 215,$

$A = (24e + 20)^2 + (31e + 26),$ $\alpha = 24e + 20\,(6, 1, 6, 48e + 41),$

$A = 426,$

$A = (63e + 27)^2 + (79e + 34),$ $\alpha = 63e + 27\,(7, 1, 7, 126e + 55),$

$A = 763,$ etc.,

$A = (5e + 1)^2 + (13e + 4),$ $\alpha = 5e + 1\,(1, 3, 1, (10e + 3),$

$A = (8e + 5)^2 + (15e + 10),$ $\alpha = 8e + 5\,(2, 3, 2, (16e + 11),$

$A = (33e + 1)^2 + (53e + 3),$ $\alpha = 33e + 1\,(3, 3, 3, (66e + 3).$

6. L'équation $\alpha^2 + \alpha - 10 = 0,$ conduit à $\alpha = 2\,(1, 2, 2, 1, 5).$

Posons

$$\alpha = a\,(1, 2, 2, 1, 2a + 1).$$

On trouve

$$5\,(\alpha^2 - a^2) + 5\alpha - (12a + 6) = 0,$$

ce qui exige qu'on prenne $a = 5e + 2.$

Alors $A = (5e + 2)^2 + 12e + 6.$

Cette formule générale donnera non seulement le développement de α pour $A = 10$ (avec $e = 0$), mais encore celui de

$A = 67, 174, 331, 538,$ etc., (avec $e = 1, 2, 3, 4,$ etc.).

7. Si on fait $A = 14,$ on trouve $\alpha = 3\,(3, 1, 1, 1, 3, 7).$

Posons $\alpha = a\,(3, 1, 1, 1, 3, 2a + 1),$

il vient $20\,(\alpha^2 - a^2) + 20\alpha - (31a + 7) = 0,$

ou avec $a = 20e + 3,$

$$\alpha^2 + \alpha - A = 0, \qquad A = (20e + 3)^2 + (31e + 5).$$

On aura ainsi pour $e = 1$

$$\alpha = 23\,(3, 1, 1, 1, 3, 47), \qquad A = 565.$$

8. Pour $A = 17$, on trouve $\alpha = 3\,(1, 1, 1, 7)$ et en général pour

$$A = 9e^2 + 7e + 1, \qquad \alpha = 3e\,(1, 1, 1, 6e + 1),$$

ce qui donne α pour

$$A = 17, 51, 103, 173, 261, 367, 491, 633, 793, 971, \text{ etc.}$$

9. $A = 18$ donne $\alpha = 3\,(1, 3, 2, 1, 1, 2, 3, 1, 7)$,

$A = 22$ $\alpha = 4\,(4, 1, 1, 1, 1, 4, 9)$,

$A = 24$ $\alpha = 4\,(2, 2, 1, 4, 4, 1, 2, 2, 9)$,

$A = 26$ $\alpha = 4\,(1, 1, 1, 1, 1, 9)$.

Ce dernier développement conduit à la formule générale

$$A = 16e^2 + 9e + 1, \qquad \alpha = 4e\,(1, 1, 1, 1, 1, 8e + 1),$$

donnant α pour

$$A = 26, 83, 172, 293, 446, 631, 848, \text{ etc.},$$

$A = 27$ donne $\alpha = 4\,(1, 2, 1, 1, 2, 1, 9)$,

$A = 28$ $\alpha = 4\,(1, 4, 2, 2, 4, 1, 9)$,

$A = 32$ $\alpha = 5\,(5, 1, 1, 2, 3, 2, 1, 1, 5, 11)$,

$A = 33$ $\alpha = 5\,(3, 1, 3, 11)$,

ce développement conduit à la formule générale

$$A = (15e + 5)^2 + (23e + 8), \qquad \alpha = (15e + 5)(3, 1, 3, 30e + 11),$$

donnant α pour $A = 33, 431$, etc.,

$A = 34$ donne $\alpha = 5\,(2, 1, 5, 5, 1, 2, 11)$,

$A = 35$ $\alpha = 5\,(2, 3, 2, 11)$ et en général

$A = (8e + 5)^2 + (15e + 10)$ donne $\alpha = 8e + 5\,(2, 3, 2, 16e + 11)$,

ce qui donne α pour

$$A = 35, 194, 481, 896, \text{ etc.}$$

$A = 37$ donne $\alpha = 5\,(1, 1, 1, 1, 11)$.

Il en résulte que si

$$A = 25e^2 + (11e + 1), \qquad \alpha = 5e\,(1, 1, 1, 1, 10e + 1),$$

ce qui donne α pour

$$A = 37,\ 123,\ 259,\ 445,\ 681,\ 967,\ \text{etc.},$$

$$A = 38 \quad \text{donne} \quad \alpha = 5\,(1, 2, 5, 1, 5, 2, 1, 11),$$

$$A = 39 \qquad \alpha = 5\,(1, 3, 3, 1, 11).$$

Si $\qquad A = (17e + 5)^2 + (43e + 14),$

on aura $\qquad \alpha = 17e + 5\,(1, 3, 3, 1, 34e + 11),$

d'où α pour $\qquad A = 39,\ 541,\ \text{etc.},$

$$A = 40 \quad \text{donne} \quad \alpha = 5\,(1, 5, 2, 2, 1, 2, 2, 5, 1, 11),$$

$$A = 44 \qquad \alpha = 6\,(6, 1, 1, 2, 1, 3, 1, 2, 1, 1, 6, 13),$$

$$A = 45 \qquad \alpha = 6\,(4, 2, 2, 4, 13),$$

$$A = 48 \qquad \alpha = 6\,(2, 4, 6, 1, 2, 1, 1, 1, 1, 2, 1, 6, 4, 3, 13),$$

$$A = 50 \qquad \alpha = 6\,(1, 1, 2, 3, 6, 1, 3, 1, 6, 3, 2, 1, 1, 13),$$

$$A = 52 \qquad \alpha = 6\,(1, 2, 1, 2, 6, 1, 6, 2, 1, 2, 1, 13),$$

$$A = 53 \qquad \alpha = 6\,(1, 3, 1, 13).$$

Le dernier développement conduit à la formule générale

$$A = (5e + 1)^2 + (13e + 4), \qquad \alpha = (5e + 1)(1, 3, 1, 10e + 3),$$

donnant α pour $\qquad A = 53,\ 151,\ 299,\ 497,\ 745,\ \text{etc.},$

$$A = 54 \quad \text{donne} \quad \alpha = 6\,(1, 6, 2, 3, 4, 1, 1, 1, 1, 1, 4, 3, 2, 6, 1, 13),$$

$$A = 58 \qquad \alpha = 7\,(7, 1, 1, 3, 3, 1, 1, 7, 15),$$

$$A = 60 \qquad \alpha = 7\,(3, 1, 4, 2, 2, 1, 1, 1, 7, 7, 1, 1, 1, 2, 2, 4, 1, 3, 15),$$

$$A = 62 \qquad \alpha = 7\,(2, 1, 1, 3, 2, 1, 7, 5, 7, 1, 2, 3, 1, 1, 2, 15),$$

$$A = 63 \qquad \alpha = 7\,(2, 4, 1, 4, 2, 15),$$

$$A = 65 \qquad \alpha = 7\,(1, 1, 2, 1, 2, 1, 1, 15),$$

$$A = 68 \qquad \alpha = 7\,(1, 3, 5, 3, 1, 15),$$

$$A = 69 \qquad \alpha = 7\,(1, 4, 1, 1, 1, 1, 4, 1, 15),$$

$$A = 70 \qquad \alpha = 7\,(1, 7, 2, 3, 1, 2, 1, 1, 2, 1, 3, 2, 7, 1, 15);$$

$A = 74$ donne $\alpha = 8\,(8, 1, 1, 3, 1, 3, 1, 1, 8, 17)$,

$A = 75$ $\alpha = 8\,(5, 1, 2, 1, 1, 1, 2, 1, 5, 17)$,

$A = 76$ $\alpha = 8\,(4, 3, 4, 17)$,

$A = 77$ $\alpha = 8\,(3, 2, 5, 2, 3, 17)$,

$A = 78$ $\alpha = 8\,(2, 1, 8, 5, 1, 3, 1, 1, 2, 2, 1, 1, 3, 1, 5, 8, 1, 2, 17)$,

$A = 80$ $\alpha = 8\,(2, 5, 2, 17)$,

$A = 82$ $\alpha = 8\,(1, 1, 3, 8, 1, 3, 1, 1, 1, 3, 1, 8, 3, 1, 1, 17)$,

$A = 84$ $\alpha = 8\,(1, 2, 8, 1, 5, 4, 2, 2, 1, 1, 1, 1, 2, 2, 4, 5, 1, 8, 2, 1, 17)$,

$A = 85$ $\alpha = 8\,(1, 2, 1, 2, 1, 17)$.

$A = 86$ $\alpha = 8\,(1, 3, 1, 2, 3, 2, 1, 3, 1, 17)$,

$A = 87$ $\alpha = 8\,(1, 5, 3, 1, 1, 3, 5, 1, 17)$,

$A = 88$ $\alpha = 8\,(1, 8, 2, 4, 4, 2, 8, 1, 17)$,

$A = 92$ $\alpha = 9\,(9, 1, 1, 4, 3, 1, 1, 1, 1, 1, 3, 4, 1, 1, 9, 19)$,

$A = 93$ $\alpha = 9\,(6, 2, 1, 1, 2, 6, 19)$,

$A = 95$ $\alpha = 9\,(3, 1, 5, 1, 3, 19)$,

$A = 96$ $\alpha = 9\,(3, 4, 1, 1, 2, 1, 2, 1, 1, 4, 3, 19)$,

$A = 97$ $\alpha = 9\,(2, 1, 3, 3, 1, 2, 19)$,

$A = 98$ $\alpha = 9\,(2, 2, 2, 1, 9, 4, 1, 5, 1, 4, 9, 1, 2, 2, 2, 19)$,

$A = 99$ $\alpha = 9\,(2, 6, 6, 2, 19)$.

Nous n'insisterons pas sur ces développements pour $A > 100$.

10. Si on cherche pour quelle valeur de A le développement α sera tel développement qu'on donne d'avance, on est conduit (T, II, p. 62), à l'équation

$$Q\,(\alpha^2 - a^2) + Q\alpha = Qa + 2Pa + (P + R),$$

qui exige qu'on ait

$$2Pa + (P + R) \equiv 0, \qquad (\text{Mod. } Q)$$

Cette congruence n'est pas possible si R et Q sont pairs (et P impair).

Mais si une combinaison quelconque se rencontre, elle se répète une infinité de fois, car si la congruence

$$2Pa + (P + R) \equiv 0, \qquad (\text{Mod. } Q)$$

est possible elle donnera une infinité de solutions pour a.

Certaines combinaisons sont toujours possibles. En particulier, la partie symétrique de la période peut être constituée de termes égaux impairs, dont le nombre est quelconque, car pour $A = a^2 + a + 1$, on a

$$\alpha = a\,(2a + 1), \qquad \text{(R, II, III, 3)}$$

ou

$$\alpha = a\,(2a + 1,\ 2a + 1,\ 2a + 1,\ \ldots,\ 2a + 1), \qquad k + 1 \text{ fois;}$$

ou

$$\alpha = a\,(\mathrm{S},\ 2a + 1),$$

S étant la partie symétrique de la période, constituée de k termes égaux à $2a + 1$.

Posons

$$\alpha = x\,(\mathrm{S},\ 2x + 1).$$

Cette équation est possible puisqu'elle a la solution

$$x = a, \qquad A = a^2 + a + 1,$$

donc elle a une infinité de solutions.

CHAPITRE V.

Équations réduites du second degré du genre hyperbole, ou équation de Pell.

1. Après avoir effectué toutes les réductions possibles, on ramène l'équation générale du second degré de genre hyperbole à l'une des deux formes suivantes

$$y^2 - Ax^2 = +1, \tag{1}$$

$$y^2 + yx - Ax^2 = +1. \tag{2}$$

Bien que l'on n'obtienne jamais les équations

$$y^2 - Ax^2 = -1, \tag{3}$$

$$y^2 + yx - Ax^2 = -1, \tag{4}$$

comme équation réduite d'une équation plus générale, nous nous occuperons également de ces dernières, leur solution étant identique à celle de (1) ou (2).

Ces équations sont appelées (à tort, paraît-il): *Équations de* PELL de première espèce (1) et (3) ou de deuxième espèce (2) ou (4).

Nous commencerons par les équations (1) et (3).

Soit donc l'hyperbole rapportée à ses axes

$$y^2 - Ax^2 = \pm 1. \tag{5}$$

A toute solution $y = b$, $x = a$ correspondent quatre solutions

$$\begin{array}{llll} y = b, & -b, & b, & -b, \\ x = a, & -a, & -a, & a. \end{array}$$

Il suffit évidemment d'en trouver une avoir pour toutes les quatre.

Géométriquement, le point (ab) en donne trois autres par symétrie (par rapport aux deux axes et par rapport au centre.

Dorénavant, quand nous parlerons d'une solution de (5), nous aurons en vue la solution positive, c'est-à-dire celle dont les deux coordonnées sont positives.

Notons enfin la solution évidente $x = 0$, $y = \pm 1$ pour l'équation (1).

2. Soit α la racine positive de l'équation

$$x^2 - A = 0, \tag{6}$$

et considérons le développement de α en fraction continue

$$\alpha = a\,(x_1, x_2, \ldots, x_k, 2a), \quad \text{(voir Chapitre II)} \tag{7}$$

Soit $\frac{b_n}{a_n}$ la réduite correspondante à l'avant-dernier quotient incomplet (donc à x_k) de la $n^{\text{ième}}$ période.

Nous allons démontrer que *les solutions*

$$y = b_n, \qquad x = a_n, \tag{8}$$

constituent toutes les solutions de (5).

D'abord (8) définit une solution de (5).

En effet, considérons la réduite

$$\frac{b_n}{a_n} = a, x_1, x_2, \ldots, x_k,$$

et la réduite $\frac{d_n}{c_n} = a, x_1, x_2, \ldots, x_{k-1}, x_k, 2a$ qui la suit.

Posons

$$z = x_1, x_2, \ldots, x_k, \ldots, \quad \text{ou} \quad \alpha = a + \frac{1}{z} = \frac{d_n z + b_n}{c_n z + a_n},$$

et en éliminant z

$$\alpha = \frac{b_n(\alpha - a) + d_n}{a_n(\alpha - a) + c_n},$$

ou enfin

$$a_n \alpha^2 + (c_n - aa_n - b_n)\,\alpha - (d_n - ab_n) = 0.$$

Cette équation devant déterminer α est identique à celle-ci

$$\alpha^2 - A = 0.$$

La comparaison des coefficients donne les équations

$$c_n - aa_n - b_n = 0,$$

$$\frac{a_n}{1} = \frac{d_n - ab_n}{A},$$

ou

$$\left.\begin{aligned} c_n &= a a_n + b_n, \\ d_n &= \mathrm{A} a_n + a b_n. \end{aligned}\right\} \quad (9)$$

Comme $\frac{d_n}{c_n}$ et $\frac{b_n}{a_n}$ sont deux réduites consécutives, on aura

$$d_n a_n - b_n c_n = (-1)^{nk+1},$$

ou

$$b_n^2 - \mathrm{A} a_n^2 = (-1)^{nk}, \quad (10)$$

ce qui prouve que les valeurs

$$y = b_n, \qquad y = a_n,$$

sont bien solution de (5).

Nous discuterons plus loin (n° 4) le signe du deuxième membre de (10).

3. Inversement, *toute solution de* (5) *peut être obtenue par les formules* (8).

Soit $x = \mathrm{Q}$, $y = \mathrm{P}$ une solution de (5), de sorte qu'on aura

$$\mathrm{P}^2 - \mathrm{AQ}^2 = \pm 1. \quad (11)$$

Soit

$$\frac{\mathrm{P}}{\mathrm{Q}} = e_0, e_1, e_2. \ldots, e_{k-1} e_k, \quad (12)$$

le développement de $\frac{\mathrm{P}}{\mathrm{Q}}$, le nombre de termes étant choisi tel que $(-1)^k$ donnera le second membre de (11).

Cela revient à dire qu'on prendra k pair si le second membre de (11) est $+1$, on prendra k impair si ce second membre est -1.

A cet effet, on remplacera, si cela est nécessaire, le dernier quotient q par $(q-1) + \frac{1}{1}$.

Soit $\frac{\mathrm{P}'}{\mathrm{Q}'}$ la réduite qui précède $\frac{\mathrm{P}}{\mathrm{Q}}$, donc

$$\frac{\mathrm{P}'}{\mathrm{Q}'} = e_0, e_1, \ldots, e_{k-1},$$

$$\mathrm{PQ}' - \mathrm{P}'\mathrm{Q} = (-1)^k = \mathrm{P}^2 - \mathrm{AQ}^2,$$

d'où

$$\frac{\mathrm{P}}{\mathrm{Q}} = \frac{\mathrm{AQ} - \mathrm{P}'}{\mathrm{P} - \mathrm{Q}'},$$

P et Q étant premiers entre eux, on aura

$$\left.\begin{aligned} AQ - P' &= lP, \\ P - Q' &= lQ, \end{aligned}\right\} \quad (13)$$

le facteur l étant entier et positif car

$$P > Q > Q' > 0.$$

Or de $\alpha^2 = A$, on tire $Q\alpha^2 + P\alpha = P\alpha + AQ$,
ou

$$\alpha = \frac{P\alpha + AQ}{Q\alpha + A},$$

ou à cause de (13)

$$\alpha = \frac{P\alpha + P' + lP}{Q\alpha + Q' + lQ} = \frac{P(\alpha + l) + P'}{Q(\alpha + l) + Q'},$$

ce qui prouve que le développement de α est

$$\alpha = e_0, e_1, e_2, \ldots, e_k, \alpha + l,$$

ou

$$\alpha = e_0, e_1, e_2, \ldots, e_k, l + e_0, e_1, e_2, \ldots.$$

Dans ce développement l'élément $l + e_0$ est un entier positif, donc ce développement est le développement ordinaire de α et est par conséquent identique à (7).

On aura donc $l + e_0 = e_{k+1} = 2e_0$, d'où $l = e_0$ et (13) s'écrit

$$\left.\begin{aligned} P' &= AQ - e_0P, \\ Q' &= P - e_0Q. \end{aligned}\right\} \quad (14)$$

4. La solution $y = b_n$, $x = a_n$ (8) de (5) satisfait à l'équation

$$b_n^2 - Aa_n^2 = (-1)^{nk}, \qquad (10)$$

Il convient actuellement de préciser le signe du second membre de (10). Par hypothèse $k + 1$ est le nombre de termes de chaque période et n le nombre de périodes.

Le signe du second membre de (10) dépend de la parité de nk et nous sommes amené à considérer les deux cas qui peuvent se présenter. Remarquons que nous disposons de la valeur de n, mais k est déterminé par la nature du développement de $\sqrt{A}$.

1° Si k est pair, le deuxième membre de (10) sera $+1$ quel que soit n. Alors, seule l'équation (1) est possible et a comme solution

$$y = b_n, \qquad x = a_n.$$

L'équation (3) est alors impossible.

Dans ce cas, la partie symétrique de la période contient *un* nombre impair de termes et il y a *un* terme du milieu de la partie symétrique, qui n'y entre qu'une seule fois.

2° Si k est impair, le signe du deuxième membre de (10) dépend de n. Dans ce cas, les deux équations (1) et (3) sont possibles.

On aura une solution de (1) en prenant n pair.

» » (3) » impair.

Dans ce cas, la partie symétrique de la période contient un nombre pair de termes, et il n'y a pas de terme du milieu, tous les termes interviennent deux fois dans la partie symétrique de la période.

Ainsi l'équation (1) est toujours possible.

C'est à cette équation que se réduit l'équation générale d'une hyperbole.

L'équation (3) n'est possible que si le développement de $\sqrt{A}$ conduit à une période constituée d'un nombre impair de termes (ou d'un nombre pair de termes dans la partie symétrique).

5. Dans certains cas, on peut à priori s'apercevoir de l'impossibilité de l'équation

$$y^2 - Ax^2 = -1. \tag{3}$$

1° On a $Ay^2 = y^2 + 1$, donc A divise une somme de deux carrés et est par conséquent aussi une somme de deux carrés. Ainsi, si l'équation $y^2 - Ax^2 = -1$, est possible, le nombre A est une somme de deux carrés.

La réciproque n'est pas vraie. Dans certains cas le nombre A est une somme de deux carrés sans que (3) soit possible.

2° On a

$$y^2 \equiv -1. \ (\text{Mod. } A)$$

Ainsi (-1) est résidu de A et de tout facteur p premier de A. Si donc A contient un ou plusieurs facteurs de la forme $4h + 3$, l'équation (3) est impossible.

Il en est en particulier ainsi pour

$$A \equiv 3,\ 6,\ 7.\ (\text{Mod. } 8)$$

3° L'équation (3) n'est pas possible si $A \equiv 0$ (Mod. 4), car alors (3) devient $y^2 \equiv -1$ (Mod. 4), ce qui n'est pas possible.

6. Formules de récurrence.

Soit $\frac{b_n}{a_n} = a, x_1, x_2, \ldots, x_{k-1}$, soit $\frac{b'_n}{a'_n}$ la réduite qui précède $\frac{b_n}{a_n}$ et calculons $\frac{b_{n+1}}{a_{n+1}}$.

On a

$$\frac{b_{n+1}}{a_{n+1}} = \frac{b_n(x_k, x_1, x_2, \ldots, x_{k-1}) + b'_n}{a_n(x_k, x_1, x_2, \ldots, x_{k-1}) + a'_n} = \frac{zb_n + b'_n}{za_n + a'_n}, \quad (15)$$

en posant

$$z = x_k, x_1, x_2, \ldots, x_{k-1}.$$

Or $\frac{b_n}{a_n}$ est la réduite qu'on obtient en arrêtant le développement de $\sqrt{A}$ un terme avant la fin de la $n^{ième}$ période donc $x_k = 2a$ et on aura

$$z = 2a, x_1, x_2, \ldots, x_{k-1}$$

$$= a + a, x_1, x_2, \ldots, x_{k+1} = a + \frac{b_1}{a_1},$$

(15) devient

$$\frac{b_{n+1}}{a_{n+1}} = \frac{\left(a + \frac{b_1}{a_1}\right) b_n + b'_n}{\left(a + \frac{b_1}{a_1}\right) a_n + a'_n} = \frac{(aa_1 + b_1) b_n + a_1 b'_n}{(aa_1 + b_1) a_n + a_1 a'_n}. \quad (16)$$

D'après (14) dans lesquelles on aura

$$P' = b'_n, \quad Q' = a'_n, \quad P = b_n, \quad Q = a_n, \quad e_0 = a,$$

et qui s'écrivent

$$b'_n = Aa_n - ab_n, \qquad a'_n = b_n - aa_n,$$

(16) devient

$$\frac{b_{n+1}}{a_{n+1}} = \frac{(aa_1 + b_1) b_n + a_1 (Aa_n - ab_n)}{(aa_1 + b_1) a_n + a_1 (b_n - aa_n)} = \frac{b_1 b_n + Aa_1 a_n}{b_1 a_n + a_1 b_n}. \quad (17)$$

Les deux termes de la dernière fraction sont premiers entre-eux, car leur diviseur commun, s'il existait, diviserait aussi

$$(b_1 b_n + \mathrm{A} a_1 a_n)\, a_1 - (b_1 a_n + a_1 b_n)\, b_1,$$

ainsi que

$$(b_1 b_n + \mathrm{A} a_1 a_n)\, b_1 - (b_1 a_n + a_1 b_n)\, \mathrm{A} a_1,$$

or, ces deux quantités se réduisent à $\pm\, a_n$ et $\pm\, b_n$ qui sont premiers entre-eux.

(17) s'écrit alors

$$\left.\begin{aligned} b_{n+1} &= b_1 b_n + \mathrm{A} a_1 a_n\,, \\ a_{n+1} &= a_1 b_n + b_1 a_n\,. \end{aligned}\right\} \quad (18)$$

Telles sont les formules de récurrence pour le calcul de b_{n+1} et a_{n+1} [1].

7. Les formules (18) donnent

$$b_{n+1} - \alpha a_{n+1} = (b_1 - \alpha a_1)\, b_n + (\mathrm{A} a_1 - \alpha b_1)\, a_n\,.$$

Or $\mathrm{A} a_1 - \alpha b_1 = -(b_1 - \alpha a_1)\,\alpha$ à cause de $\alpha^2 = \mathrm{A}$ et la formule précédente devient

$$\begin{aligned} b_{n+1} - \alpha a_{n+1} &= (b_1 - \alpha a_1)\, b_n - (b_1 - \alpha a_1)\, \alpha a_n \\ &= (b_1 - \alpha a_1)\,(b_n - \alpha a_n)\,. \end{aligned}$$

On aura ainsi

$$\begin{aligned} b_n - \alpha a_n &= (b_1 - \alpha a_1)\,(b_{n-1} - \alpha a_{n-1}), \\ b_{n-1} - \alpha a_{n-1} &= (b_1 - \alpha a_1)\,(b_{n-2} - \alpha a_{n-2}), \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ b_2 - \alpha a_2 &= (b_1 - \alpha a_1)^2, \end{aligned}$$

---

(1) On remarque que ces formules peuvent être résolues par rapport aux variables a_n, b_n. On trouve

$$a_n = \mp\,(a_1 b_{n+1} - b_1 a_{n+1}),$$

$$b_n = \pm\,(b_1 b_{n+1} - \mathrm{A} a_1 a_{n+1}).$$

et en faisant le produit de ces égalités

$$b_n - \alpha a_n = (b_1 - \alpha a_1)^n \text{ (1)}. \tag{19}$$

Ainsi, la solution $y = b_1$, $x = a_1$ est la solution *primitive* ou *fondamentale* de l'équation (5). Toute autre solution en dérive par (18) ou (19).

8. La formule (19) subsiste pour toutes les valeurs entières de n.

Pour $n = 0$, on trouve la solution évidente $y = 1$, $x = 0$.

Soit n négatif et posons $n = -m$, alors

$$b_n - \alpha a_n = (b_1 - \alpha a_1)^n = (b_1 - \alpha a_1)^{-m} = \frac{(b_1 + \alpha a_1)^m}{(b_1 - \alpha a_1)^m (b_1 + \alpha a_1)^m}$$

$$= \frac{(b_1 + \alpha a_1)^m}{b_1^2 - \mathrm{A} a_1^2} = \frac{(b_1 + \alpha a_1)^m}{\pm 1} = \pm (b_1 + \alpha a_1)^m = \pm (b_m + \alpha a_m).$$

Ainsi

$$b_n - \alpha a_n = \pm (b_m + \alpha a_m),$$

de même

$$b_n + \alpha a_n = \pm (b_m - \alpha a_m),$$

ce qui donne

$$b_n = \pm b_m, \qquad \text{ou} \qquad b_{-m} = \pm b_m,$$

$$a_n = \mp a_m, \qquad a_{-m} = \mp a_m.$$

Dans ces formules n est négatif et m positif

$$n = -m.$$

Comme on le voit, il n'est d'aucune utilité de considérer les valeurs négatives de n. On obtient ces résultats en donnant à n les valeurs positives et en prenant les solutions symétriques d'une solution donnée.

---

(1) La formule (19) peut être vérifiée plus simplement comme suit.

Posons

$$y - \alpha x = (b_1 - \alpha a_1)^n. \tag{19bis}$$

on aura en remplaçant α par $-\alpha$

$$y + \alpha x = (b_1 + \alpha a_1)^n,$$

et en multipliant membre à membre, on aura à cause de $\alpha^2 = \mathrm{A}$

$$y^2 - \mathrm{A} x^2 = (b_1^2 - \mathrm{A} a_1^2)^n,$$

et puisque $(a_1 b_1)$ est une solution de (5), (x, y) définis par (19bis) sont aussi une solution de (5).

Exemples.

1° $A = 23, \quad \alpha = 4, 1, 3, 1, 8, 1, 3, 1, 8.$

L'équation $y^2 - 23x^2 = -1,$ n'est pas possible.

On trouve

$$\frac{b_1}{a_1} = 4, 1, 3, 1 = \frac{24}{5}, \quad \text{d'où} \quad \frac{b_1}{24} = \frac{a_1}{5} = 1.$$

Les solutions de

$$y^2 - 23x^2 = +1,$$

sont

$$(y - \alpha x) = (24 - 5\alpha)^n.$$

$A = 0$ donne $y = 1, \quad x = 0$ (solution évidente),

$A = 1 \quad y = 24, \quad x = 5$ (solution primitive ou fondamentale),

$A = 2 \quad y = 1151, \quad x = 240,$ etc.

2° $A = 41, \quad \alpha = 6, 2, 2, 12, 2, 2, 12, \ldots..$

Chacune des équations $y^2 - 41x^2 = +1$ ou -1 est possible.

On a

$$\frac{b_1}{a_1} = 6, 2, 2 = \frac{6 \,|\, 13 \,|\, 32}{1 \,|\, 2 \,|\, 5}$$

$$\frac{b_1}{32} = \frac{a_1}{5} = 1.$$

Ces valeurs vérifient l'équation

$$b^2 - 41a^2 = -1.$$

On a

$$(32 - 5\alpha)^2 = 2049 - 320\alpha.$$

Cela étant, considérons séparément les deux équations

1° L'équation $y^2 - 41x^2 = -1,$

a la solution primitive (fondamentale),

$$y = 32, \quad x = 5,$$

et une infinité de solutions (x, y) données par

$$y - \alpha x = (32 - 5\alpha)^{2k+1}$$
$$= (32 - 5\alpha)(2049 - 320\alpha)^k.$$

2° L'équation

$$y^2 - 41x^2 = +1,$$

a la solution primitive (fondamentale)

$$y = 2049, \qquad x = 320,$$

et une infinité de solutions données par la formule

$$y - \alpha x = (2049 - 320\alpha)^k = (32 - 5\alpha)^{2k}.$$

9. Occupons nous maintenant des équations

$$y^2 + xy - \mathrm{A}x^2 = +1, \tag{2}$$

et

$$y^2 + xy - \mathrm{A}x^2 = -1, \tag{4}$$

que nous écrirons

$$y^2 + xy - \mathrm{A}x^2 = \pm 1. \tag{20}$$

On peut répéter, à propos de cette équation, à peu près tout ce que nous avons dit de l'équation (5).

Nous nous contenterons d'énoncer les théorèmes suivants qu'on démontre comme leurs analogues.

1° *Le développement de la racine positive de l'équation*

$$z^2 + z - \mathrm{A} = 0,$$

est indéfiniment périodique. Un seul terme précède la partie périodique. Soit *e* ce terme.

Le dernier terme de chaque période est 2e + 1.

Si on fait abstraction de ce terme, ce qui reste de la période est symétrique.

2° Soit $\frac{b_n}{a_n}$ la réduite obtenue en arrêtant le développement un terme avant la fin de la $n^{ième}$ période. *Les solutions*

$$y = b_n, \qquad x = a_n,$$

constituent toutes les solutions positives de (20) et inversement, *toute solution de* (20) *peut être obtenue par ces formules.*

3° En dehors de la solution évidente $y = 1$, $x = 0$, à chaque solution $y = b$, $x = a$, correspondent quatre solutions associées

$$x = a, \quad -a, \quad -a, \quad a,$$

$$y = b, \quad -b, \quad a + b, \quad -(a + b).$$

Ce sont les coordonnées d'un point entier M et de ses trois symétriques (par rapport au centre et par rapport aux deux axes).

4° Les solutions $y = b_n$, $x = a_n$ vérifient l'équation

$$b_n^2 + a_n b_n - \mathrm{A} a_n^2 = (-1)^{nk},$$

$k + 1$ étant le nombre des termes dans la période et n le nombre des périodes.

Si k est pair, seule l'équation (2), dont le deuxième nombre est $+1$ a des solutions, l'équation (4) dont le deuxième membre est -1 est impossible.

Si k est impair, les deux équations envisagées sont possibles. On aura les solutions de la première en prenant n pair et celles de la deuxième avec n impair.

5° Les formules de récurrence sont

$$\left.\begin{aligned} b_{n+1} &= b_1 b_n + \mathrm{A} a_1 a_n, \\ a_{n+1} &= a_1 b_n + (b_1 + a_1)\, a_n, \end{aligned}\right\} \quad (21)$$

ou

$$b_n - \alpha a_n = (b_1 - \alpha a_1)^n, \quad (22)$$

α étant cette fois racine de l'équation

$$\alpha^2 + \alpha - \mathrm{A} = 0.$$

Les formules (21) et (22) subsistent pour toutes les valeurs entières de n.

6° Dans certains cas on ramène (20) à (5).

Si A est pair, l'équation (20) exige que x soit pair et y impair.

Posons alors

$$y = y' - x', \qquad x = 2x',$$

(20) devient

$$y'^2 - (4A + 1)\, x'^2 = \pm 1.$$

10. Soit $ay^2 + 2bxy + cx^2 = 1$, une équation qui se ramène à $t^2 - Au^2 = 1$ (T, II, p. 26-27) par la substitution modulaire que nous avons envisagée.

Soit x_0, y_0 une solution particulière de

$$ay^2 + 2bxy + cx^2 = 1.$$

Soit (t_1, u_1) la solution fondamentale (primitive) de l'équation

$$t^2 - Au^2 = 1,$$

et désignons par z et α, les racines positives des équations

$$az^2 + 2bz + c = 0, \qquad \alpha^2 - A = 0.$$

Comme on a

$$A = b^2 - ac, \qquad \text{(T, II, p. 27)}$$

on aura

$$\alpha = az + b.$$

Soit maintenant (x, y) une solution quelconque de

$$ay^2 + 2bxy + cx^2 = 1,$$

(t, u) une solution quelconque de

$$t^2 - Au^2 = 1,$$

et considérons l'expression

$$y - zx,$$

qui devient par la substitution modulaire envisagée (T, II, p 27)

$$y - zx = (y_0 - zx_0)\, t - [(b + za)\, y_0 + (c + zb)\, x_0]\, u.$$

Or

$$az^2 + 2bz + c = 0, \qquad \text{donne} \qquad (az + b)\, z + (bz + c) = 0,$$

ou

$$(bz + c) = - z\,(az + b),$$

et l'expression précédente devient

$$\begin{aligned} y - zx &= (y_0 - zx_0)\,t - [(b + za)\,y_0 - (az + b)\,x_0 z]\,u \\ &= (y_0 - zx_0)[t - (az + b)\,u] = (y_0 - zx_0)(t - \alpha u) \\ &= (y_0 - zx_0)(t_1 - \alpha u_1)^n \text{ (1)}, \end{aligned} \tag{23}$$

n étant un entier arbitraire.

Ainsi donc, partant d'une solution particulière $(x_0 y_0)$ de l'équation

$$ay^2 + 2bxy + cx^2 = 1,$$

et d'une solution fondamentale $(t_1 u_1)$ de

$$t^2 - \mathrm{A}u^2 = 1,$$

$(\mathrm{A} = b^2 - ac)$, on aura toutes les solutions (xy) de l'équation

$$ay^2 + 2bxy + cx^2 = 1,$$

par la formule

$$y - zx = (y_0 - zx_0)\,(t_1 - \alpha u_1)^n,$$

---

(1) Si on pose

$$y - zx = (y_0 - zx_0)\,(t_1 - \alpha u_1)^n,$$

on aura en remplaçant z et α par z', $-\alpha$, z' étant la racine conjuguée de z

$$y - z'x = (y_0 - z'x_0)\,(t_1 + \alpha u_1)^n,$$

ou en multipliant par la précédente

$$(y - zx)(y - z'x) = (y_0 - zx_0)\,(y_0 - z'x_0)\,(t_1 - \alpha u_1)^n\,(t_1 + \alpha u_1)^n.$$

ou bien, en multipliant par a

$$ay^2 + 2bxy + cx^2 = (ay_0^2 + 2bx_0y_0 + cx_0^2)\,(t_1^2 - \mathrm{A}u_1^2)^n,$$

et puisque (x_0, y_0) est solution de $ay^2 + 2bxy + cx^2 = 1$, et $(t_1\, u_1)$ solution de $t^2 - \mathrm{A}u^2 = 1$, on aura

$$ay^2 + 2bxy + cx^2 = 1,$$

ce qui prouve que (23) définit une solution.

z et α étant racines des équations

$$az^2 + 2bz + c = 0, \qquad \alpha^2 - A = 0.$$

De même, si le coefficient de xy est impair, on aura une solution générale de l'équation

$$ay^2 + (2b + 1)\, xy + cx^2 = 1,$$

en partant d'une solution particulière $(x_0 y_0)$ de cette équation, et d'une solution fondamentale $(t_1 u_1)$ de l'équation

$$t^2 + tu - Au^2 = 1, \qquad (A = b^2 + b - ac),$$

par la formule

$$y - zx = (y_0 - zx_0)\,(t_1 - \alpha u_1)^n,$$

z et α étant racines des équations

$$az^2 + (2b + 1)\, z + c = 0, \qquad \alpha^2 + \alpha - A = 0.$$

11. Une autre équation, qui se comporte à peu près comme celle de Pell, est l'équation indéterminée

$$x^2 - Ay^2 = \pm D \; (D^2 < A).$$

Elle n'est possible que si D figure parmi le dénominateur des quotients complets. Supposons qu'il en soit ainsi.

A moins que D ne soit le dénominateur du quotient incomplet correspondant au milieu de la partie symétrique, ce dénominateur se rencontrera au moins deux fois dans le courant d'une période. Il en résulte que l'équation

$$x^2 - Ay^2 = \pm D,$$

peut avoir plusieurs solutions fondamentales.

Le signe du second membre de l'équation

$$x^2 - Ay^2 = \pm D,$$

dépend du rang du quotient complet, dont le dénominateur est D. Si cependant le nombre de termes de la période est impair, on

trouvera ce quotient complet à un rang de parité voulue dans l'une ou l'autre période.

Enfin, nous remarquerons que comme précédemment d'une solution $(x_0 y_0)$ donnée, on tire une infinité de solutions par les formules de récurrence

$$x - \sqrt{A}\, y = (x_0 - \sqrt{A}\, y_0)(t_1 - \sqrt{A}\, u_1)^n,$$

$(t_1 u_1)$ étant la solution (la plus petite si on veut) de l'équation de Pell

$$x^2 - Ay^2 = +1.$$

DEUXIÈME PARTIE.

L'Arithmétique des formes quadratiques.

CHAPITRE VI.

Généralités sur les formes.

1. Définitions. — Nous appellerons *forme* tout polynome homogène. Les formes se classent :

1° Suivant le nombre des variables en

formes à *une* variable,

» *deux* variables ou *binaires*,

» *trois* » *ternaires*, etc.

2° Suivant le degré en

formes du premier degré ou linéaires,

» deuxième » quadratiques,

» troisième » cubiques,

» quatrième » bi-quadratiques, etc.

Nous ferons une étude *arithmétique* des formes binaires et quadratiques. Nous supposerons donc que les coefficients sont des entiers, et que les variables ne peuvent recevoir que des valeurs entières. On écrira la forme f sous la forme

$$f = ax^2 + bxy + cy^2. \tag{1}$$

Nous écrirons $f(abc)$ quand il s'agira de mettre en évidence les trois coefficients de la forme. Nous écrirons $f(xy)$ quand il s'agira de mettre en évidence les indéterminées x et y. Enfin, nous écrirons simplement f quand aucune confusion ne sera à craindre.

Nous appellerons *déterminant* de la forme f la quantité

$$\Delta = b^2 - 4ac.$$

La forme sera dite *primitive* si a, b et c sont premiers entre eux. On dit que le nombre N est *représentable* par la forme f si on peut trouver des valeurs entières x_0, y_0 telles que

$$ax_0 + bx_0y_0 + cy_0 = \mathrm{N}.$$

La représentation $x = x_0$, $y = y_0$, est primitive (ou propre) si x_0 et y_0 sont premiers entre eux.

Il est évident que le déterminant est de même parité que b.

2. Substitutions linéaires. — Par définition, *effectuer dans la forme f une substitution linéaire* $\mathrm{D}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, *c'est remplacer x et y par $\alpha x' + \beta y'$ et $\gamma x' + \delta y'$.*

Dans l'arithmétique des formes, on ne considère que les substitutions entières c'est-à-dire, telles que α, β, γ, δ sont des entiers.

La quantité $\mathrm{D} = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = \alpha\delta - \beta\gamma$ est le déterminant de la substitution.

Si on effectue la substitution D dans la forme f, on trouve

$$f' = (a\alpha^2 + b\alpha\gamma + c\gamma^2)\, x'^2 + [2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta]\, x'y' \\ + (a\beta^2 + b\beta\delta + c\delta^2)\, y^2.$$

Le déterminant de la nouvelle forme est

$$\Delta' = [2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta]^2 \\ - 4(a\alpha^2 + b\alpha\gamma + c\gamma^2)(a\beta^2 + b\beta\delta + c\delta^2),$$

on trouve

$$\Delta' = (\alpha\delta - \beta\gamma)^2 (b^2 - 4ac). \qquad (2)$$

Nous supposerons toujours $\mathrm{D} \neq 0$, (2) s'écrit $\Delta' = \mathrm{D}^2\Delta$.

Nous dirons que la forme f renferme f', ou bien que la forme f' est contenue dans f.

Ainsi, si la forme f renferme f', le déterminant de f' est divisible par le déterminant de f et le quotient est un carré parfait.

Tout nombre représentable par f' l'est aussi par f, car à tout système des valeurs entières de x' et y' correspondent des valeurs entières de x et y. Mais la réciproque n'est pas vraie.

La substitution

$$\left.\begin{aligned} x &= \alpha x' + \beta y', \\ y &= \gamma x' + \delta y', \end{aligned}\right\} \quad (3)$$

définit x', y' en fonction de x et y par les formules

$$\left.\begin{aligned} Dx' &= \delta x - \beta y, \\ Dy' &= -\gamma x + \alpha y. \end{aligned}\right\} \quad (4)$$

Les valeurs de x' et y' seront entières si $D = \pm 1$.

On est ainsi amené à la considération des substitutions spéciales, telles que $D = \pm 1$.

3. Produit de deux substitutions.

Si dans la forme f on fait la substitution $D\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, on trouve la forme f'. Effectuons dans cette dernière la substitution $D'\begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}$. On trouvera une forme f''.

Il est évident qu'on peut passer directement de f à f'' par une substitution unique que nous allons déterminer.

On aura par D

$$x = \alpha x' + \beta y',$$
$$y = \gamma x' + \delta y',$$

et par D'

$$x' = \alpha' x'' + \beta' y'',$$
$$y' = \gamma' x'' + \delta' y'',$$

ce qui donne

$$\begin{aligned} x &= \alpha(\alpha' x'' + \beta' y'') + \beta(\gamma' x'' + \delta' y'') \\ &= (\alpha\alpha' + \beta\gamma')\, x'' + (\alpha\beta' + \beta\delta')\, y', \\ y &= \gamma(\alpha' x'' + \beta' y'') + \delta(\gamma' x'' + \delta' y'') \\ &= (\gamma\alpha' + \gamma'\delta)\, x'' + (\beta'\gamma + \delta\delta')\, y'', \end{aligned}$$

et la substitution unique pour passer de f à f'' est

$$DD'\begin{pmatrix} \alpha\alpha' + \beta\gamma' & \alpha\beta' + \beta\delta' \\ \gamma\alpha' + \gamma'\delta & \beta'\gamma + \delta\delta' \end{pmatrix},$$

dont le déterminant est

$$DD' = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} \cdot \begin{vmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{vmatrix} = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} \begin{vmatrix} \alpha' & \gamma' \\ \beta' & \delta' \end{vmatrix}.$$

On dis que la substitution DD′ est le produit des deux substitutions D et D′.

4. Substitution inverse.

Si, en partant des formules (4), on considère la substitution

$$D^{-1} \begin{pmatrix} \dfrac{+\delta}{D} & \dfrac{-\beta}{D} \\ \dfrac{-\gamma}{D} & \dfrac{+\alpha}{D} \end{pmatrix},$$

on dira que c'est une substitution inverse de D. Si $D = \pm 1$. la substitution inverse, déterminée ainsi, permettrait de passer de f' à f. Mais si $D \neq \pm 1$, on ne considérera pas la substitution inverse, ses coefficients étant alors fractionnaires.

Une substitution sera dite *modulaire* si $D = +1$.

Si le déterminant d'une substitution est -1, multiplions-la par $\begin{vmatrix} 1 & 0 \\ 0 & -1 \end{vmatrix}$, et on aura une autre substitution dont le déterminant sera $+1$.

On sera ainsi amené à considérer les substitutions *modulaires*.

Parmi les substitutions modulaires, retenons les suivantes :

1° Les substitutions identiques

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad I' = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Si on effectue ces substitutions sur une forme f donnée, elle reste inchangée.

Une telle substitution est dite *automorphe*.

2° La substitution $T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, dont l'effet est de changer la forme

$$f = ax^2 + bxy + cy^2, \qquad \text{en} \qquad f' = cx^2 - bxy + ay^2.$$

On voit qu'on change le signe du second terme, ainsi que l'ordre des coefficients.

3° La substitution $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, et celles qui en dérivent

$$S^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \qquad S^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \text{ etc.,}$$

et en général

$$S^m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}.$$

La forme f devient

$$f = a(x + my)^2 + b(x + my)y + cy^2$$
$$= ax^2 + (2am + b)xy + (am^2 + bm + c)y^2.$$

Si la substitution D par laquelle on passe de f à f' est telle que $D = \pm 1$, les formes f et f' sont équivalentes.

Elles sont proprement équivalentes si $D = +1$ (quand la substitution est modulaire) et improprement équivalente, si $D = -1$.

Chacune des deux formes équivalentes contient l'autre, ou bien tout nombre représentable par l'une des deux formes équivalentes, l'est aussi par l'autre.

Deux formes équivalentes ont le même déterminant.

Car la formule (2) devient si $D = \pm 1$, $\Delta' = \Delta$.

Mais, *la réciproque n'est pas vraie*, c'est-à-dire *deux formes de même déterminant ne sont pas nécessairement équivalentes.*

Ainsi, les formes $x^2 + 6y^2$ et $2x^2 + 3y^2$ ont le même déterminant -6, mais ne sont pas équivalentes, car les nombres premiers à six représentables par la première forme sont $\equiv 1$ (Mod. 6) et ceux représentables par la deuxième sont $\equiv 5$ (Mod. 6).

Dans la suite, nous nous occuperons exclusivement des substitutions modulaires.

Les formes auxquelles on les applique sont proprement équivalentes et appartiennent à une même *classe*. On appelle *classe* de formes, toutes les formes qui se déduisent de l'une d'elles par des substitutions modulaires.

5. Théorème. — *Si* N *est représentable par* f, Δ *est résidu quadratique de* N.

En effet, soit

$$N = ax^2 + bxy + cy^2,$$

ou

$$4a\mathrm{N} = (2ax + by)^2 - (b^2 - 4ac)\, y^2 = (2ax + by)^2 - \Delta y^2.$$

Ou

$$(2ax + by)^2 \equiv \Delta y^2, \qquad (\text{Mod. N})$$

Le produit de deux facteurs $(2ax + by)^2$ et l'un de ces facteurs y^2 étant résidu, l'autre facteur Δ l'est aussi.

6. Problème. — Le nombre N étant de la forme f, résoudre la congruence

$$u^2 \equiv \Delta. \qquad (\text{Mod. N}).$$

La formule

$$(2ax + by)^2 \equiv \Delta y^2, \qquad (\text{Mod. N}).$$

trouvée précédemment, donne

$$\left(\frac{2ax + by}{y}\right)^2 \equiv \Delta \equiv u^2, \qquad (\text{Mod. N}).$$

d'où

$$u \equiv \pm \frac{2ax + by}{y}, \qquad (\text{Mod. N}). \qquad (\text{T, p. 25-26})$$

On peut expliciter cette solution comme suit :

Posons $zx - ty = 1$, x et y étant solutions de

$$\mathrm{N} = ax^2 + bxy + cy^2.$$

L'identité

$$4f(xy)\, f(tz) = [z\,(bx + 2cy) + t\,(2ax + by)]^2 - \Delta\,(zx - ty)^2,$$

devient

$$[z\,(bx + 2cy) + t\,(2ax + by)]^2 \equiv \Delta, \qquad (\text{Mod. N})$$

ce qui donne

$$u \equiv \pm\, [z\,(bx + 2cy) + t\,(2ax + by)]. \qquad (\text{Mod. N})$$

7. Théorème. — Pour qu'un entier N puisse être primitivement représenté par une forme f de classe C, il faut et il suffit qu'il existe dans cette classe une forme dont le premier coefficient est N.

Cette condition est nécessaire. En effet, si on peut trouver deux entiers p, q, tels que

$$f(pq) = ap^2 + bpq + cq^2 = \mathrm{N},$$

faisons dans f une substitution modulaire $D\begin{pmatrix} p & \alpha \\ q & \beta \end{pmatrix}$, (en déterminant préalablement deux nombres α et β, tels que $p\beta - q\alpha = +1$), alors f devient f', dont le premier coefficient est

$$a' = ap^2 + bpq + cq^2, \qquad \text{ou} \qquad N.$$

Cette condition est suffisante, car, si elle est vérifiée la forme f est $Nx^2 + bxy + cy^2$, et devient N avec $x = 1$, $y = 0$.

8. L'équation

$$az^2 + bz + c = 0,$$

sera dite équation caractéristique de la forme $f(a, b, c)$.

Si les racines de l'équation caractéristique sont imaginaires, la forme ne peut représenter que les nombres de même signe (celui de a ou c). Mais si les racines de l'équation caractéristique sont réelles et inégales, la forme peut représenter tous les nombres depuis $-\infty$ jusqu'à $+\infty$.

La forme f est un carré parfait, si $\Delta = 0$, alors les racines de l'équation caractéristique sont égales.

Nous ne nous occuperons provisoirement pas des formes dans lesquelles $\Delta = 0$.

La forme f est définie, si $\Delta < 0$. Elle est indéfinie, si $\Delta > 0$.

La forme définie f est positive, si $a > 0$ (alors $c > 0$). Elle est négative, si a (ainsi que c) < 0.

9. Soit $u \equiv u_0$ (Mod. N), une solution de la congruence $u^2 \equiv \Delta$ (Mod. N), que nous avons trouvée au numéro 6 de ce chapitre. On aura

$$u_0^2 - \Delta = Np, \qquad \text{ou} \qquad 4Np,$$

il en résulte que la forme

$$f(N, u_0, p),$$

a comme déterminant

$$u^2 - 4Np = \Delta,$$

et elle représente primitivement le nombre N avec $x = 1$, $y = 0$.

Cela étant, désignons par $u_1, u_2, u_3, \ldots$, différentes solutions de

la congruence $u^2 \equiv \Delta$ (Mod. N) [1], et soient p_1, p_2, p_3 les entiers définis par

$$p_1 = \frac{n_1^2 - \Delta}{4N}, \qquad p_2 = \frac{n_2^2 - \Delta}{4N}, \qquad \ldots.$$

L'entier N est représentable dans les classes

$$f_1\,(N,\ n_1,\ p_1), \qquad \text{et} \qquad f_2\,(N,\ n_2,\ p_2), \qquad \ldots.$$

Une forme $f(a, b, c)$ étant donnée, si parmi les différentes formes $f_1, f_2, \ldots$, on en trouve une qui soit de la même classe f, le nombre peut être représenté par f. Si aucune forme f_i n'est de la même classe que f, la représentation $f = N$ n'est pas possible.

Soit $D\begin{pmatrix} \alpha_0 & \beta_0 \\ \gamma_0 & \delta_0 \end{pmatrix}$ la substitution qui transforme f en f_i et $S\begin{pmatrix} \lambda & m \\ \nu & p \end{pmatrix}$ une substitution automorphe de f, alors toutes les substitutions transformant f en f_1 sont données par DS.

Leur nombre est fini, si la forme f est définie et infini dans le cas des formes indéfinies.

---

(1) Si N n'est pas premier, la congruence $u^2 \equiv \Delta$ (Mod. N) peut avoir plus de deux solutions.

CHAPITRE VII.

Formes quadratiques définies.

1. Une forme définie positive $f = ax^2 + bxy + cy^2$ sera dite *réduite*, si les conditions suivantes sont remplies

$$-a < b \leqslant a \leqslant c, \tag{1}$$

et si $\quad a = c, \quad$ on doit avoir $\quad b \geqslant 0. \tag{2}$

2. Problème. — Réduire une forme (définie positive) donnée.

Cela revient à trouver une forme proprement équivalente à la forme donnée et dans laquelle les deux conditions (1) sont vérifiées, en supposant que (1) ou (2) ne soient pas vérifiées dans la forme donnée. Les inégalités (1) peuvent s'écrire $|b| \leqslant a$, $a \leqslant c$.

A cet effet, nous démontrerons que par certaines *substitutions modulaires*, on peut graduellement transformer la forme donnée en vue de satisfaire aux conditions (1) ou (2).

On peut supposer que dans la forme donnée $a \leqslant c$.

S'il n'en n'est pas ainsi, appliquons à f la substitution $T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ dont l'effet est de changer l'ordre des coefficients (ainsi que le signe de b, mais ceci est sans grande importance).

Si donc $a \leqslant c$, mais si la première inégalité (1) n'est pas vérifiée, appliquons à f la substitution $S^m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$, f devient

$$ax^2 + (2am + b)\,xy + (am^2 + bm + c)\,y^2,$$

et déterminons m par la condition

$$|2am + b| < |a|.$$

Si dans la nouvelle forme obtenue toutes les inégalités (1) sont vérifiées, elle est réduite. Dans le cas contraire, la première inégalité sera vérifiée et la deuxième pas.

Alors, on appliquera à nouveau la substitution $T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et on continuera ainsi jusqu'à ce que les deux inégalités (1) soient vérifiées.

Reste la condition (2), si la forme obtenue n'y satisfait pas, soit $f(a, -b, a) = ax^2 - bxy + ay^2$, cette forme, elle devient $f(a, b, a) = ax^2 + bxy + ay^2$, par la substitution $T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et (2) sera satisfaite.

3. Théorème. — Si la forme $f = ax^2 + bxy + cx^2$ est réduite, on aura

$$|\Delta| \geqslant 3a^2, \tag{3}$$

l'égalité n'ayant lieu que si $a = b = c$.

En effet, on a $\Delta = b^2 - 4ac < 0$, puisqu'il s'agit d'une forme définie, donc $|\Delta| = 4ac - b^2 \geqslant 0$. En tenant compte des inégalités (1) et (2), on trouve (3).

4. Théorème. — Deux formes réduites ne peuvent être de même classe sans être identiques.

Soit $f(abc)$ et $f'(a'b'c')$, deux formes de même classe et soit $D\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ la substitution par laquelle on passe de la première à la seconde. On aura

$$\left.\begin{aligned} a' &= a\alpha^2 + b\alpha\gamma + c\gamma^2, \\ b' &= 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta, \\ c' &= a\beta^2 + b\beta\delta + c\delta^2, \\ D &= \alpha\delta - \beta\gamma = +1. \end{aligned}\right\} \tag{4}$$

La première des égalités (4) donne

$$4aa' = (2a\alpha + b\gamma)^2 + \Delta\gamma^2. \tag{5}$$

Or, les deux formes f et f' étant réduites, on aura $|\Delta| \geqslant 3a^2$, et $|\Delta'| \geqslant 3a'^2$. Supposons $a' \leqslant a$, alors $|\Delta| > 3aa'$, et (5) donnera

$$(2a\alpha + b\gamma)^2 = 4aa' - \Delta\gamma^2 \leqslant |\Delta| \left(\frac{4}{3} - \gamma^2\right),$$

relation qui prouve que $\gamma = 0$ ou ± 1, Examinons ces deux cas.

1° Si $\gamma = 0$, on aura par (4), $D = \alpha\delta = 1$, ce qui donne $\alpha = \delta = \pm 1$. On peut se borner à examiner le cas de $\alpha = \delta = +1$[1]. Les autres équations (4) donnent alors

$$a' = a, \qquad b' = 2a\beta + b, \qquad c' = a\beta^2 + b\beta + c. \tag{6}$$

Les deux formes f et f' étant réduites, on aura

$$-a < b \leqslant a, \qquad -a' < b' \leqslant a',$$

ou (puisque $a' = a$) $\qquad -a < b' \leqslant a,$

ou encore $\qquad -2a < b' - b < 2a.$

Par suite, la deuxième égalité (6), donne $2a\beta = b' - b < |2a|$, d'où $\beta = 0$, alors $b' = b$ et $c' = c$, ce qui donne $f' = f$, et les deux formes sont identiques.

2° Si $\gamma = \pm 1$, on peut prendre $\gamma = +1$ [1]. On peut encore supposer $a' \leqslant a$.

(5) donne alors

$$(2a\alpha + b\gamma)^2 = 4aa' - \Delta\gamma^2,$$

ou

$$(2a\alpha + b)^2 = 4aa' - \Delta,$$

et comme

$$|\Delta| \geqslant 3a^2 \qquad \text{ou} \qquad \geqslant 3aa',$$

on aura

$$(2a\alpha + b)^2 \leqslant a^2. \tag{7}$$

Comme la forme f est réduite, on aura $|b| < |a|$ et (7) donne $\alpha = 0$ ou ± 1.

1° Si $\alpha = 0$ (et $\gamma = +1$), (4) donne $\beta = -1$, $a' = c$, $2c\delta = b' + b$, or les deux formes étant réduites

$$-a' - a < b' + b < a' + a \qquad \text{ou} \qquad |b' + b| \leqslant |2c|,$$

d'où $\delta = 0$ ou ± 1.

Si $\delta = 0$, $D = \begin{vmatrix} 0 & -1 \\ 1 & 0 \end{vmatrix}$.

---

[1] Si par $D = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix}$, on transforme de f en f', on le fait aussi par $D = \begin{vmatrix} -\alpha & -\beta \\ -\gamma & -\delta \end{vmatrix}$.

Les deux formes ne diffèrent que par le signe du second terme et de plus, comme $a = c$, ces formes sont

$$f = ax^2 + bxy + cy^2, \qquad f' = ax^2 - bxy + cy^2.$$

Elles ne sont réduites, toutes les deux, que si $b = 0$. Alors elles sont identiques.

Si $\delta = 1$, $D = \begin{vmatrix} 0 & -1 \\ 1 & 1 \end{vmatrix}$, $b' = 2a - b$, $c' = 2a - b$.

Les deux formes sont alors

$$f = ax^2 + bxy + ay^2, \qquad f' = ax^2 + (2a - b)\,xy + (2a - b)\,y^2,$$

f' étant réduite, on aura $2a - b < a$ ou $a \leqslant b$, mais comme $b \leqslant a$, on aura $a = b$. Alors les deux formes sont identiques $f(a, a, a)$.

Si $\alpha = 1$ ($\gamma = 1$), on trouve par (4)

$$a' = a + b + c,$$

égalité impossible, si les deux formes sont réduites.

Enfin, $\alpha = -1$ ($\gamma = 1$), conduit à prendre (4)

$$a' = a - b + c,$$

et comme $a' \leqslant a$, on aura

$$b \geqslant c \qquad \text{ou} \qquad b \leqslant a \leqslant c,$$

donc $a = b = c$ et la première forme f est $f(a, a, a)$.

La première des égalités (4), donne alors $a' = a$, la seconde donne

$$a(\delta - \beta) = b',$$

et comme

$$|b'| \leqslant |a'| \leqslant |a|,$$

on aura

$$\delta - \beta = 0 \qquad \text{ou} \qquad 1.$$

La dernière équation (4), donne $\delta + \beta = -1$, il faut donc prendre $\delta - \beta = 1$ (et non 0), alors $\delta = 0$, $\beta = -1$, et D devient $\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$. Elle transforme $f(a, a, a)$, en elle-même.

Dans ce cas encore les deux formes sont identiques.

5. Problème. — Étant données deux formes définies de même déterminant, déterminer si elles sont de même classe.

On réduira chacune des formes données. Si les deux formes réduites sont identiques, elles sont de même classe.

Dans le cas contraire, elles sont de classes différentes.

On trouvera dans le premier cas, la substitution pour passer de l'une à l'autre de la façon suivante :

Soit D la substitution qui transforme f en sa réduite.

» D′ » » f' »

La substitution $D.D'^{-1}$ transformera f en f'.

Exemples. 1° $f = 593x^2 - 1340xy + 757y^2$,

$$f' = 4069x^2 + 4332xy + 1153y^2.$$

Par la substitution

$D_1 \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, f devient $f_1 = 593x^2 - 154xy + 10y^2$,

$D_2 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, f_1 $f_2 = 10x^2 + 154xy + 593y^2$,

$D_3 \begin{pmatrix} 1 & -8 \\ 0 & 1 \end{pmatrix}$, f_2 $f_3 = 10x^2 - 6xy + y^2$,

$D_4 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, f_3 $f_4 = x^2 + 6xy + 10y^2$,

$D_5 \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix}$, f_4 $f_5 = x^2 + y^2$.

La dernière forme est la forme réduite de f.

On passe de f à f_5 par une seule substitution

$$D = D_1D_2D_3D_4D_5 = \begin{pmatrix} -9 & 26 \\ -8 & 23 \end{pmatrix}.$$

On réduira de même la forme f'.

Par $D'_1 \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, f' devient $f'_1 = 4069x^2 - 3806xy + 890y^2$,

$D'_2 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, f'_1 $f'_2 = 890x^2 + 3806xy + 4069y^2$,

UNIVERSITAS SCIENTIAE

Par $D'_3\begin{pmatrix}1 & -2\\ 0 & 1\end{pmatrix}$, f'_2 devient $f'_3 = 890x^2 + 246xy + 17y^2$,

$D'_4\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$, f'_3 $\qquad f'_4 = 17x^2 - 246xy + 890x^2$,

$D'_5\begin{pmatrix}1 & +7\\ 0 & 1\end{pmatrix}$. f'_4 $\qquad f'_5 = 17x^2 - 8xy + y^2$,

$D'_6\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$, f'_5 $\qquad f'_6 = x^2 + 8xy + 17y^2$,

$D'_7\begin{pmatrix}1 & -4\\ 0 & 1\end{pmatrix}$, f'_6 $\qquad f'_7 = x^2 + y^2$.

On passe de f' à f'_2 par une seule substitution

$$D' = D'_1D'_2D'_3D'_4D'_5D'_6D'_7 = \begin{pmatrix}-8 & 33\\ 15 & -62\end{pmatrix}.$$

Les deux formes réduites de f et f' étant identiques, f et f' sont de la même classe.

On passe de f à f' par une substitution DD'^{-1}.

L'inverse de D' est

$$D'^{-1}\begin{pmatrix}62 & 33\\ 15 & 8\end{pmatrix}, \qquad \text{et} \qquad DD'^{-1} = \begin{pmatrix}168 & 89\\ 151 & 80\end{pmatrix}.$$

Par cette dernière substitution f devient f'.

2° Soit $\qquad f = 358x^2 + 816xy + 465y^2$,

$$f' = 206x^2 + 476xy + 275y^2.$$

Par $D_1\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}$, f devient $f_1 = 358x^2 + 100xy + 7y^2$,

$D_2\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$, f_1 $\qquad f_2 = 7x^2 - 100xy + 358y^2$,

$D_3\begin{pmatrix}1 & +7\\ 0 & 1\end{pmatrix}$, f_2 $\qquad f_3 = 7x^2 - 2xy + y^2$,

$D_4\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$, f_3 $\qquad f_4 = x^2 + 2xy + 7y^2$,

$D_5\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}$, f_5 $\qquad f_6 = x^2 + 6y^2$.

C'est la forme réduite. On passe de f à f_6 par une seule substitution

$$D_1D_2D_3D_4D_5 = D = \begin{pmatrix} -8 & 9 \\ 7 & -8 \end{pmatrix}.$$

Pour la réduction de f', on prendra d'abord

La substitution

$D'_1 \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, et f' deviendra $f'_1 = 206x^2 + 64xy + 5y^2$,

puis

$D'_2 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, f'_1 $f'_2 = 5x^2 - 64xy + 206y^2$,

puis

$D'_3 \begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix}$, f'_2 $f'_3 = 5x^2 - 4xy + 2y^2$,

puis

$D'_4 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, f'_3 $f'_4 = 2x^2 + 4xy + 5y^2$,

enfin

$D'_5 \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, f'_4 $f'_5 = 2x^2 + 3y^2$.

On passe de f' à f'_5 par une seule substitution

$$D' = D'_1D'_2D'_3D'_4D'_5 = \begin{pmatrix} -7 & 8 \\ 6 & -7 \end{pmatrix},$$

f' et f'_5 étant toutes deux réduites et non identiques, les deux formes f et f' ne sont pas de la même classe, bien qu'elles soient du même déterminant $\Delta = -6$.

6. Substitution automorphe d'une forme définie.

Les substitutions $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $I' = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ sont évidemment automorphes. Voyons s'il existe d'autres substitutions automorphes.

Soit $D = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ une substitution (modulaire) automorphe. On aura

$$\left.\begin{aligned} \alpha\delta - \beta\gamma &= +1, \\ a\alpha^2 + b\alpha\gamma + c\gamma^2 &= a, \\ 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta &= b. \end{aligned}\right\} \quad (8)$$

La dernière équation, en tenant compte de le première équation (8), s'écrit

$$2a\alpha\beta + 2b\beta\gamma + 2c\gamma\delta = 0.$$

Cette équation et les deux premières (8) donnent

$$\left.\begin{aligned} a\beta + c\gamma &= 0, \\ a(\alpha - \delta) + \beta\gamma &= 0, \end{aligned}\right\}$$

ou

$$\frac{+\beta}{-c} = \frac{\gamma}{a} = \frac{\alpha - \delta}{-\beta} = u, \tag{9}$$

u étant la valeur commune de ces rapports.

Soit d le plus grand commun diviseur des coefficients de la forme (donc $d = 1$, si la forme est primitive).

Remplaçons dans (9) u par $\frac{u}{d}$, il viendra

$$\left.\begin{aligned} \beta &= -\frac{c}{d}u, \\ \gamma &= \frac{a}{d}u, \\ \alpha - \delta &= \frac{-\beta}{d}u. \end{aligned}\right\} \tag{10}$$

Pour que α, β, γ et δ soient entiers, il faut que u le soit. Si dans $\alpha\delta - \beta\gamma = 1$, on remplace α, β, γ et δ par leurs valeurs (10), on trouve

$$\alpha\delta + \frac{ac}{d^2}u^2 = 1, \quad \text{ou} \quad \frac{(\alpha+\delta)^2 - (\alpha-\delta)^2}{4} + \frac{ac}{d^2}u^2 = 1,$$

ou

$$\left(\frac{\alpha+\delta}{2}\right)^2 - \left(\frac{b}{2d}u\right)^2 + \frac{ac}{d^2}u^2 = 1,$$

$$\left(\frac{\alpha+\delta}{2}\right)^2 + \frac{\Delta}{4d^2}u^2 = 1,$$

ce que nous écrirons

$$[d(\alpha+\delta)]^2 + \Delta u^2 = 4d^2,$$

ou enfin

$$t^2 + \Delta u^2 = 4d^2, \tag{11}$$

en posant $\qquad t = d(\alpha + \delta).$

Ces quantités, t, u et d étant supposées connues, on aura

$$\alpha = \frac{t - bu}{2d}, \qquad \beta = \frac{-cu}{d}, \qquad \gamma = \frac{au}{d}, \qquad \delta = \frac{t + bu}{2d}. \quad (12)$$

Inversement, si on détermine les solutions entières (t, u) de (11) et quatre nombres entiers $(\alpha, \beta, \gamma, \delta)$ par (12) la substitution $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, est automorphe.

7. Si $d = 1$, c'est-à-dire, si la forme est primitive, l'équation (11) devient

$$t^2 + \Delta u^2 = 4,$$

dont la seule solution est

$$t = \pm 2, \qquad u = 0, \qquad (\text{si } |\Delta| > 4),$$

et les substitutions correspondantes sont

$$\alpha = \pm 1 = \delta, \qquad \beta = \gamma = 0,$$

ce qui donne les deux substitutions automorphes connues

$$\mathrm{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \text{et} \qquad \mathrm{I}' = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Dans ce cas, il n'y en a pas d'autres.

Toutefois, si $b = 0$, on aura les substitutions automorphes

$$\mathrm{T} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \mathrm{TI}' = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Comme deuxième cas particulier, considérons le cas $a = b = c$, c'est-à-dire, le cas de la forme

$$f = ax^2 + axy + ay^2,$$

qui, en dehors des substitutions automorphes I et I', a encore les suivantes

$$\mathrm{TS} = \mathrm{D} = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \qquad \mathrm{DI}' = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix},$$

$$\mathrm{D}^{-1} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \qquad \text{et} \qquad \mathrm{D}^{-1}\mathrm{I}' = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}.$$

Si $d \neq 1$, il peut exister d'autres substitutions automorphes.

Il résulte de ce qui précède que toute forme définie primitive autre que $f(1, 0, 1)$ et $f(1, 1, 1)$, n'a pas d'autres substitutions automorphes que I et I'.

La forme $f(1, 0, 1)$, a encore les substitutions automorphes T et TI'.

Enfin, la forme $f(1, 1, 1)$, a les substitutions automorphes suivantes I, I', TS = D, DI', D^{-1}, $D^{-1}I'$.

8. Nous achèverons la théorie des formes définies par la solution de la question suivante :

Étant donné un déterminant négatif donné, trouver toutes les formes définies ayant ce déterminant.

Soit Δ le déterminant donné, on aura $3a^2 < |\Delta|$ et aussi $3b^2 < |\Delta|$.

Cela étant, considérons toutes les valeurs de b, *de même parité que* Δ, satisfaisant à cette inégalité. Elles sont en nombre fini. Pour chacune de ces valeurs de b, on calculera le nombre $4ac = b^2 - \Delta$, qu'on décomposera de toutes les manières possibles en deux facteurs qui déterminerons a et $c > a$.

On obtiendra ainsi toutes (en nombre fini) les formes réduites ayant le déterminant donné.

Cela revient à trouver toutes les solutions (en nombre fini) de l'équation indéterminée en a, b, c

$$\Delta = b^2 - 4ac.$$

On remarquera que certaines valeurs ne peuvent pas être prises pour Δ.

Ainsi $\Delta = b^2 - 4ac < 0$, ne peut être en valeur absolue $\equiv 1$ ou 2 (Mod. 4), car cela donnerait $b^2 \equiv 3$ ou 2 (Mod. 4), congruence impossible.

Exemples. 1° $\Delta = -3$. La seule valeur de b à considérer est $b = 1$, donc $ac = 1$, d'où $a = c = 1$, et la seule forme de ce déterminant est $f = x^2 + xy + y^2 = f(1, 1, 1)$.

2° $\Delta = -4$, $b = 0$, donne $ac = 1$, d'où $a = c = 1$,

et $$f = f(1, 0, 1) = x^2 + y^2.$$

3° $\Delta = -7$, $b = 1$, $ac = 2$, d'où $a = 1$, $c = 2$;

$$f = f(1, 1, 2) = x^2 + xy + 2y^2.$$

4° $\Delta = -8$, $b = 0$, $ac = 2$, d'où $a = 1$, $c = 2$,

$$f = f(1, 0, 2) = x^2 + 2y^2.$$

5° $\Delta = -11$, $b = 1$, $ac = 3$, d'où $f = x^2 + xy + 3y^2$.

6° $\Delta = -12$, $b = 0$, $ac = 3$, $f = x^2 + 3y^2$.

$$2, \qquad 4, \quad a = c = 2,$$

$$f = 2x^2 + 2xy + 2y^2.$$

Dans ce cas f n'est pas une forme primitive, car Δ étant divisible par le carré de deux, f est divisible par deux.

7° $D = 15$, $b = 1$, $ac = 4$, $a = c = 2$, $f = 2x^2 + xy + 2y^2$,

$$a = 1, \ c = 4, \qquad x^2 + xy + 4y^2.$$

9. Représentation géométrique.

Toute forme $f = ax^2 + bxy + cy^2$ peut être réduite en une autre $f' = a'x'^2 + b'x'y' + c'y'^2$ par des substitutions modulaires et la nouvelle forme satisfera aux conditions

$$-a' < b' \leqslant a' \leqslant c', \qquad (\text{ou} \qquad a' = c' \geqslant b' > 0),$$

Soient

$$az^2 + bz + c, \qquad \text{et} \qquad a'z'^2 + b'z' + c' = 0,$$

les équations caractéristiques de ces formes.

On aura

$$z = \frac{-b \pm \sqrt{-\Delta}}{2a}, \qquad z' = \frac{-b' \pm \sqrt{-\Delta'}}{2a'}.$$

D'abord pour préciser le double signe du radical, nous allons considérer la racine qu'on obtient en prenant le signe + devant le radical, aussi bien dans z que dans z'.

On écrira alors

$$z = u + ti, \qquad z' = u' + t'i,$$

étant posé

$$u = -\frac{b}{2a}, \qquad u' = -\frac{b'}{2a'}, \qquad t = \frac{\sqrt{-\Delta}}{2a}, \qquad t' = \frac{\sqrt{-\Delta}}{2a'}.$$

La forme f' étant réduite, on aura $-a' < b' < a'$, ou en divisant par $2a'$

$$-\frac{1}{2} < u' < +\frac{1}{2}. \tag{1}$$

On trouve encore que le module

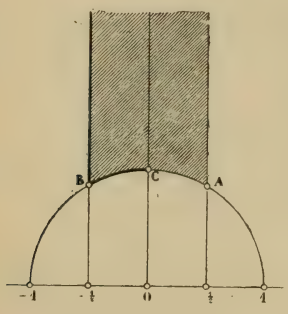
$$|z'| = \sqrt{u'^2 + t'^2} = \sqrt{\left(\frac{-b'}{2a'}\right)^2 + \frac{-\Delta'}{4a^2}}$$

$$= \sqrt{\frac{b^2 + 4ac - b^2}{4a^2}} = \sqrt{\frac{c}{a}} \geqslant 1. \tag{2}$$

Cela étant, voici comment on peut interpréter géométriquement la réduction des formes quadratiques définies.

Convenons de représenter géométriquement la valeur de $z = u + ti$ par le point z de coordonnées (u, t).

Alors (1) exprime que z' se trouve entre les deux parallèles à OC d'abscisses $+\frac{1}{2}$ et $-\frac{1}{2}$.



(2) Exprime que le point z' est à l'extérieur du cercle de rayon OA $= 1$.

Ainsi, si la forme f est réduite, le point z de la racine de son équation caractéristique se trouve :

1° Entre les deux parallèles à OC.

2° En dehors du cercle BCA.

Le point z se trouvera ainsi à l'intérieur du triangle curviligne TBA (le point T étant rejeté à l'infini dans la direction OC).

Pour tenir compte du cas limite ($a = c$, $b > 0$), nous dirons que si le point z figuratif de la racine z de l'équation, est sur le périmètre de ce triangle, il doit être sur la moitié gauche (négative) de ce périmètre.

Le triangle curviligne TBA (la moitié gauche du périmètre comprise) sera dit *Domaine fondamental.*

Tout point du plan est de même classe qu'un point et un seul du domaine fondamental.

Dans le domaine fondamental, il n'y a pas deux points qui soient de même classe.

Cet énoncé correspond à celui que nous avons vu (p. 96), que deux formes réduites ne peuvent être de même classe sans être identiques.

CHAPITRE VIII.

Formes quadratiques indéfinies.

1. Nous nous occuperons maintenant des formes $f = ax^2 + bxy + cy^2$ indéfinies, c'est-à dire, telle que $\Delta = b^2 - 4ac > 0$, mais non carré parfait. Si en effet, Δ est le carré parfait de d, f se décompose en deux formes linéaires et on aura

$$4af = (2ax + by)^2 - d^2y^2 = [2ax + (b + d)\,y][2ax + (b - d)\,y].$$

2. Forme réduite.— Une forme indéfinie $f = ax^2 + bxy + cy^2$ sera dite réduite, si la plus grande racine de son équation caractéristique se développe en fraction continue périodique simple.

Les deux racines de l'équation caractéristique

$$az^2 + bz + c = 0,$$

étant

$$z_1 = \frac{-b + \sqrt{\Delta}}{2a}, \qquad \text{et} \qquad z_2 = \frac{-b - \sqrt{\Delta}}{2a},$$

les conditions pour qu'une forme f soit réduite, peuvent s'écrire

$$z_1 > 1, \qquad -1 < z_2 < 0, \qquad \text{(T, II, p. 13)}$$

ce qui donne, $f(z)$ désignant le premier membre de l'équation caractéristique et a étant supposé positif

$$f(-1) > 0, \qquad f(0) < 0, \qquad f(1) < 0,$$

ou

$$a > 0, \qquad a - b + c > 0, \qquad a + b + c < 0, \qquad c < 0.$$

Remarquons que dans le cas de formes indéfinies, deux formes réduites ne sont pas nécessairement identiques, contrairement à ce qui a eu lieu pour les formes définies.

3. Problème. — Réduire une forme donnée.

Soit $f(a, b, c)$ la forme donnée et ω_1 la plus grande racine de son équation caractéristique.

On développera ω_1 en fraction continue. On trouve

$$\omega_1 = a_1, a_2, a_3, \ldots, a_k (b_1, b_2, \ldots, b_n),$$

les a_i étant les quotients incomplets qui précèdent la période et les b_j étant les quotients incomplets qui forment la période.

On s'arrangera d'abord pour que le nombre de termes qui précède la période, soit pair. On commencera, à cet effet, la période à partir de b_1, si k est pair et à partir de b_2, si k est impair. Cela étant, soit z la période

$$z = (b_1, b_2, \ldots, b_n), \text{ si } k \text{ est pair,}$$

$$z = (b_2, b_3, \ldots, b_n, b_1), \text{ si } k \text{ est impair,}$$

$$\omega_1 = a_1, a_2, a_3, \ldots, a_{2i}, z, \qquad \text{ou} \qquad \omega_1 = \frac{p_{2i}z + p_{2i-1}}{q_{2i}z + q_{2i-1}}.$$

De plus, la substitution $D = \begin{pmatrix} p_{2i} & p_{2i-1} \\ q_{2i} & q_{2i-1} \end{pmatrix}$ est modulaire et z étant une fraction continue périodique simple, la forme qui lui correspond est réduite.

D'ailleurs, rien n'empêche de commencer la période 2, 4, 6, 8, 10, ... termes plus loin. Donc, à moins que n ne soit égale à 1 ou 2, il y aura plusieurs (mais un nombre limité) formes réduites équivalentes à la proposée.

4. Il est facile de préciser le nombre des formes réduites de la même classe qu'une forme donnée. On peut d'abord s'arranger pour que la période soit constituée d'un nombre pair de termes, en prenant, si cela est nécessaire, deux périodes pour une.

Soit donc $2h$ le nombre de termes de la période.

Soit

$$z = (a_1, a_2, a_3, a_4, \ldots, a_{2h}),$$

le développement de la racine positive de l'équation caractéristique de la forme réduite.

Les développements

$$z_1 = (a_1, a_2, a_3, \ldots, a_{2h}),$$

$$z_2 = (a_3, a_4, \ldots, a_{2h}, a_1, a_2),$$

$$a_3 = (a_5, a_6, \ldots, a_3, a_4),$$

$$\cdots\cdots\cdots\cdots$$

$$a_i = (a_{2i-1}, a_{2i}, \ldots, a_{2i-2}),$$

$$\cdots\cdots\cdots\cdots$$

$$a_h = (a_{2h-1}, a_{2h}, \ldots, a_{2h-2}),$$

conduiront aux h formes réduites de la même classe que la forme proposée.

5. Cherchons les substitutions automorphes d'une forme réduite donnée.

Soit

$$z = (a_1, a_2, a_3, \ldots, a_{2h}),$$

le développement de la racine positive de l'équation caractéristique, ce développement, comprenant un nombre $(2h)$ pair de termes. On prendra comme précédemment deux périodes pour une, si cela est nécessaire.

On aura

$$x = \frac{p_{2h}x + p_{2h-1}}{q_{2h}x + q_{2h-1}},$$

il en résulte que la substitution $A\begin{pmatrix} p_{2h} & p_{2h-1} \\ q_{2h} & q_{2h-1} \end{pmatrix}$ est une substitution (modulaire) automorphe.

On obtient encore des substitutions automorphes, en prenant $4h$, $6h$, $8h$, ..., termes dans la période.

Soit

$$A_2 = \begin{pmatrix} p_{4h} & p_{4h-1} \\ q_{4h} & q_{4h-1} \end{pmatrix}, \quad A_3 = \begin{pmatrix} p_{6h} & p_{6h-1} \\ q_{6h} & q_{6h-1} \end{pmatrix}, \quad \ldots, \quad A_k = \begin{pmatrix} p_{2kh} & p_{2kh-1} \\ q_{2kh} & q_{2kh-1} \end{pmatrix},$$

ces substitutions. Comme dans le cas de l'équation de Pell, on démontrera que

1° Ce sont là toutes les substitutions automorphes.

2° On a $\qquad A_k = A^k, \qquad$ (T, II, p. 79).

D'ailleurs, en suivant la voie indiquée pour les formes définies, on trouve qu'une substitution $D\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ sera automorphe, si α, β, γ et δ sont définis par les formules (T, II, p. 103)

$$\alpha = \frac{t - bu}{d}, \qquad \beta = \frac{cu}{d}, \qquad \gamma = \frac{au}{d}, \qquad \delta = \frac{t + bu}{d},$$

t et u satisfaisant à l'équation de Pell

$$t^2 - \Delta u^2 = d^2,$$

dont nous nous sommes occupé au Chapitre V.

6. Une autre question qui se pose à propos des formes indéfinies, est la suivante. Un déterminant positif étant donné, trouver toutes les formes réduites des différentes classes ayant ce déterminant.

La question sera résolue par les inégalités que nous avons établies

$$a > 0, \quad c < 0, \quad a + b + c < 0, \quad a - b + c > 0, \text{ (T. II, p. 108).}$$

Les deux dernières exigent qu'on ait

$$b < 0, \qquad \text{et} \qquad (a + c)^2 - b^2 < 0, \qquad \text{ou} \qquad (a + c)^2 < b^2.$$

Cette dernière inégalité donne, en tenant compte de

$$\Delta = b^2 - 4ac > 0,$$

$$(a + c)^2 + b^2 - 4ac < b^2 + \Delta,$$

ou

$$(a - c)^2 < \Delta,$$

et comme

$$a > 0, \qquad c < 0, \qquad a - c \quad \text{sera} \quad > 0,$$

et on aura simplement

$$a - c < \sqrt{\Delta},$$

et à fortiori

$$a < \sqrt{\Delta}.$$

Ainsi, on examinera toutes les valeurs positives de a inférieures à $\sqrt{\Delta}$, toutes les valeurs négatives de c depuis -1 jusqu'au $-(a-\sqrt{\Delta})$, a et c étant choisis, on aura

$$b = -\sqrt{\Delta + 4ac}.$$

On ne gardera que les solutions dans lesquelles a et c sont tels que b est rationnel.

Ces inégalités seront toujours compatibles, car de telles formes existent toujours (par exemple la forme $f = x^2 - \Delta y^2$).

Il restera à reconnaître lesquelles des formes réduites sont de même classe.

CHAPITRE IX.

Formes quadratiques binaires, binomes, définies.

1. Une des plus intéressantes applications de la théorie qui précède est l'étude des formes binomes, c'est-à-dire, le cas où $b = 0$.

Si la forme est réduite, on aura $a \leqslant c$. Nous supposerons de plus que a et c sont premiers entre eux, c'est-à-dire, que la forme est primitive. Dans la troisième partie de cet ouvrage, on s'occupera de la résolution effective de l'équation $ax^2 + cy^2 = N$.

Pour le moment nous allons étudier certaines propriétés de cette forme.

2. Considérons d'abord *toutes* les formes réduites ayant un déterminant Δ (< 0) donné.

Elles sont en nombre fini, et constituent autant de classes qu'il y a des formes, puisqu'il n'y en a pas deux qui soient équivalentes.

Ainsi $\Delta = -15$, donne les deux classes

$$f_1(1, 1, 4) = x^2 + xy + 4y^2,$$

$$f_2(2, 1, 2) = 2x^2 + xy + 2y^2. \qquad \text{(T, II, p. 105)}$$

Ainsi, toute forme dont le déterminant est -15 est équivalente, soit à f_1, soit à f_2. S'il n'y a qu'une seule classe, aucune question ne se pose, Par exemple, pour $\Delta = -4$, la forme réduite est $f = x^2 + y^2$ et on a cet énoncé simple :

Toute forme dont le déterminant est -4 est équivalente à la forme $x^2 + y^2$.

De même, si $\Delta = -3$, $f = x^2 + xy + y^2$. Il en résulte que toute forme dont le déterminant est -3, est équivalente à la forme $f = x^2 + xy + y^2$.

Nous allons apporter la précision nécessaire dans le cas, ou il y a plus d'une classe de formes réduites.

3. Considérons les deux classes

$f_1 = f(1,1,4) = x^2 + xy + 4y^2$, et $f_2 = f(2,1,2) = 2x^2 + xy + 2y^2$,

du déterminant $\Delta = -15$. Soit N un nombre représentable par f_1 ou f_2 et considérons le reste de N pour le module Δ ou plutôt pour 3 et 5 qui entrent comme facteurs dans Δ.

On trouve

$$f_1 = x^2 + xy + 4y^2 \equiv (x - y)^2, \qquad \text{(Mod. 3)}$$

$$f_2 = 2x^2 + xy + 2y^2 \equiv 2\,(x + y)^2.$$

Il en résulte que si on excepte les nombres $N \equiv 0$ (Mod. 3), on aura

$$f_1 \equiv 1, \qquad f_2 \equiv 2 \text{ (Mod. 3)},$$

ou bien

$$\left(\frac{f_1}{3}\right) = +1, \qquad \left(\frac{f_2}{3}\right) = -1.$$

De même, pour le module 5, on aura

$$f_1 = x^2 + xy + 4y^2 \equiv (x - 2y)^2, \qquad \text{(Mod. 5)}$$

$$f_2 = 2x^2 + xy + 2y^2 \equiv 2\,(x - y)^2.$$

Donc à l'exception des nombres $N \equiv 0$ (Mod. 5), on aura

$$\left(\frac{f_1}{5}\right) \equiv +1, \qquad \left(\frac{f_2}{5}\right) \equiv -1.$$

Cela étant, nous pouvons préciser le cas d'une forme d'un déterminant égale à -15 de la façon suivante :

Soit f une forme dont le déterminant est -15.

La forme f est équivalente, soit à $f_1\,(1,1,4)$, soit à $f_2\,(2,1,2)$. La forme f est équivalente à f_1, si on a

$$\left(\frac{N}{3}\right) = \left(\frac{N}{5}\right) = +1, \text{ et à } f_2 \text{ si } \left(\frac{N}{3}\right) = \left(\frac{N}{5}\right) = -1,$$

N étant un nombre quelconque représentable par cette forme.

Si un nombre N premier à 30 est représentable par la forme f dont le déterminant est -15, on aura $\left(\frac{-15}{N}\right) = +1$, donc N doit être de la forme $30k + 1, 17, 19, 23$. Il y a lieu de distinguer deux cas.

1° $N \equiv 1$, ou 19 (Mod. 30), alors $\left(\frac{N}{3}\right) = \left(\frac{N}{5}\right) = +1$, et la forme est équivalente à f_1.

2° $N \equiv 17$, ou 23, alors $\left(\frac{N}{3}\right) = \left(\frac{N}{5}\right) = -1$, et la forme est équivalente à f_2.

On peut énoncer ce résultat autrement :

Tout nombre premier de la forme linéaire $30k + 1$, 19 (ou tout nombre composé de facteurs premiers de la forme $30k + 1$, 19), peut être représenté par une forme f de déterminant -15, équivalente à $f_1 = x^2 + xy + 4y^4$.

Tout nombre premier de la forme linéaire $30k + 17$, 23 (ou tout nombre composé de facteurs premiers de la forme $30k + 17$, 23) peut être représenté par une forme f de déterminant -15, équivalente à $f_2 = 2x^2 + xy + 2y^2$.

4. Quand il y aura plusieurs formes réduites de même déterminant, on appellera *caractères*, les signes distinctifs de chacune des formes réduites. Ces caractères seront établis :

1° Pour chacun des facteurs premiers entrant comme facteur dans Δ.

2° Dans certains cas, pour le nombre 4 ou 8.

On appellera *genre*, l'ensemble des formes ayant les mêmes caractères. Pour traiter un exemple numérique, considérons les formes réduites des déterminants $\Delta = -644 = 4.7.23$.

On aura les réduites suivantes :

$b = 0$,	$ac = 161$,	$a = 1$,	$c = 161$,	$f_1 = f(1, 0, 161)$,
		$a = 7$,	$c = 23$,	$f_2 = f(7, 0, 23)$,
$b = 2$,	$ac = 162$,	$a = 2$,	$c = 81$,	$f_3 = f(2, 2, 81)$,
		$a = 3$,	$c = 54$,	$f_4 = f(3, \pm 2. 54)$,
		$a = 6$,	$c = 27$,	$f_5 = f(6, \pm 2, 27)$,
		$a = 9$,	$c = 18$,	$f_6 = f(9, \pm 2, 18)$,
$b = 4$,	$ac = 165$,	$a = 5$,	$c = 33$,	$f_7 = f(5, \pm 4, 33)$,
		$a = 11$,	$c = 15$,	$f_8 = f(11, \pm 4, 15)$,

$b = 6, \quad ac = 170, \quad a = 10, \quad c = 17, \quad f_9 = f(10, \pm 6, 17).$

$b = 8, \quad ac = 177,$ aucune solution,

$b = 10, \quad ac = 186,$ »

$b = 12, \quad ac = 197,$ »

$b = 14, \quad ac = 210, \quad a = 14, \quad c = 15, \quad f_{10} = f(14, 14, 15).$

On a ainsi les 10 (ou 16) formes réduites f_i ($i = 1$ à 10).

Si on représente par N_i un nombre représentable par f_i.

On aura

$$\left(\frac{N_i}{7}\right) = +1, \quad \left(\frac{N_i}{23}\right) = +1, \quad \text{pour } i = 1, 3, 6, \quad \text{alors } N_i \equiv 1 \pmod{4}$$

$$\left(\frac{N_i}{7}\right) = -1, \quad \left(\frac{N_i}{23}\right) = -1, \quad \text{pour } i = 7, 9, \quad \text{alors } N_i \equiv 1 \pmod{4}$$

$$\left(\frac{N_i}{7}\right) = +1, \quad \left(\frac{N_i}{23}\right) = -1, \quad \text{pour } i = 2, 8, 10, \quad \text{alors } N_i \equiv 3 \pmod{4}$$

$$\left(\frac{N_i}{7}\right) = -1, \quad \left(\frac{N_i}{23}\right) = +1, \quad \text{pour } i = 4, 5, \quad \text{alors } N_i \equiv 3 \pmod{4}$$

Ainsi pour $\Delta = -644$, on aura quatre genres comprenant chacun deux ou trois classes. Chaque genre comprend quatre classes, si on tient compte du double signe de b quand $a > b$.

5. Dans les formes *binomes*, on aura $b = 0$; dans ce cas il est commode d'introduire le déterminant $d = \frac{1}{4}\Delta = -ac$.

Nous considérerons spécialement, dans ce paragraphe, le cas où il y a autant de genres que de classes, et une classe par genre.

Soit, pour fixer les idées, $\Delta = -7392$, $d = -1848$.

Voici d'abord les seize réduites

$b = 0, \quad ac = 1848, \quad a = 1, \quad c = 1848, \quad i = 1, \quad f_1 = f(1, 0, 1848),$

$a = 3, \quad c = 616, \quad i = 2, \quad f_1 = f(3, 0, 616),$

$a = 7, \quad c = 264, \quad i = 3, \quad f_1 = f(7, 0, 264),$

$a = 8,\ c = 231,\ i = 4,\ f_1 = f(8, 0, 231),$

$a = 11,\ c = 168,\ i = 5,\ f_1 = f(11, 0, 168),$

$a = 21,\ c = 88,\ i = 6,\ f_1 = f(21, 0, 88),$

$a = 24,\ c = 77,\ i = 7,\ f_1 = f(24, 0, 77),$

$a = 33,\ c = 56,\ i = 8,\ f_1 = f(33, 0, 56),$

$b = 2,\ ac = 1849,\ a = 43,\ c = 43,\ i = 9,\ f_1 = f(43, 2, 43),$

$b = 4,\ i = 10,\ f_1 = f(4, 4, 463),$

$b = 6,$ acune solution,

$b = 8,\ a = 8,\ c = 233,\ i = 11,\ f_1 = f(8, 8, 233),$

$b = 10,$ aucune solution,

$b = 12,\ a = 12,\ c = 157,\ i = 12,\ f_1 = f(12, 12, 157),$

$b = 14,$ aucune solution,

$b = 16,$ »

$b = 18,$ »

$b = 20,$ »

$b = 22,$ »

$b = 24,\ a = 24,\ c = 83,\ i = 13,\ f_1 = f(24, 24, 83),$

$b = 26,$ aucune solution,

$b = 28,\ a = 28,\ c = 73,\ i = 14,\ f_1 = f(28, 28, 73),$

$b = 38,\ a = 47,\ c = 47,\ i = 15,\ f_1 = f(47, 38, 47),$

$b = 44,\ a = 44,\ c = 53,\ i = 16,\ f_1 = f(44, 44, 53).$

Cherchons les caractères de ces seize réduites pour les modules 3, 7, 11 et 8. Nous désignons dans la table qui suit, par $+$ le symbole $\left(\frac{f_i}{p}\right) = +1$, ($p = 3$, 7 ou 11), et par $-$ le symbole $\left(\frac{f_i}{p}\right) = -1$, ($p = 3$, 7 ou 11). Nous donnons ensuite la valeur de r dans $f_i \equiv r$ (Mod. 8), i variant de 1 à 16.

i,	$\left(\frac{f_i}{3}\right)$	$\left(\frac{f_i}{7}\right)$	$\frac{f_i}{11}$	$f_i \equiv r_i$ (Mod. 8)
1	+	+	+	1
2	+	—	+	3
3	+	—	—	7
4	—	+	—	7
5	—	+	+	3
6	+	+	—	5
7	—	—	—	5
8	—	—	+	1
9	+	+	—	3
10	+	+	+	7
11	—	+	—	1
12	+	—	+	5
13	—	—	—	3
14	+	—	—	1
15	—	—	+	7
16	—	+	+	5

On voit par cette analyse, qu'il n'y a pas deux classes qui aient les mêmes caractères. Il en résulte que tout nombre premier N dont $\Delta = -1848$ est résidu, est représentable par une des seize réduites. Il en est de même d'un nombre N composé de facteurs premiers, tels que $\Delta = -1848$ est résidu de chacun. Dans ce cas, il existe plusieurs représentations du nombre par cette forme.

En pratique, quand on désire appliquer ces formes à la factorisation, il n'est pas nécessaire de considérer toutes les seize réduites (dont la moitié sont des formes trinomes), il suffit de considérer l'une d'elle, la première par exemple $f = x^2 + 1848y^2$. On aura cet énoncé.

Si le nombre N est tel $\left(\frac{N}{3}\right) = \left(\frac{N}{7}\right) = \left(\frac{N}{11}\right) = +1$, et $N \equiv +1$ (Mod. 8).

Si, de plus, la représentation $x^2 + 1848y^2$ est possible d'une seule façon, le nombre N est premier. Si la représentation $x^2 + 1848y^2$ n'est pas possible, ou bien, si elle est possible de plusieurs façons, le nombre N est composé.

Dans le premier cas (si la représentation $N = x^2 + 1848y^2$ n'est pas possible), les facteurs de N sont tels que les relations

$$\left(\frac{N}{3}\right) = \left(\frac{N}{7}\right) = \left(\frac{N}{11}\right) = +1, \quad \text{et} \quad N \equiv +1 \ (\text{Mod. } 8)$$

ne sont pas toutes vérifiées pour ces facteurs. Dans le deuxième cas, elles le sont.

On peut former un énoncé semblable pour la deuxième forme, ainsi que pour chacune des suivantes. Mais nous n'insisterons pas sur ce point.

6. Le déterminant $\Delta = -1848$ n'est pas le seul qui jouisse de la propriété remarquable, de ne donner lieu qu'à une seule classe par genre.

Nous donnons ci-dessous, d'après Euler dans la classification de Gauss [1], les soixante-cinq valeurs connues de Δ, ayant cette propriété.

1° $-\frac{\Delta}{4} = d = 1, 2, 3, 4, 7.$

2° 5, 6, 8, 9, 10, 12, 13, 15, 16, 18, 22, 25, 28, 37, 58.

3° 21, 24, 30, 33, 40, 42, 45, 48, 57, 60, 70, 72, 78, 85, 88, 93, 102, 112, 130, 133, 177, 190, 232, 253.

4° 105, 120, 165, 168, 210, 240, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760.

5° 840, 1320, 1365, 1848.

Pour toutes ces valeurs de Δ, on aura une classe par genre, mais le nombre total de classes (ou de genres est un pour 1°, deux pour 2°, quatre pour 3°, huit pour 4° et seize pour 5°.

---

(1) Gauss Disquis, n° 303. Ces valeurs de Δ sont dites par Euler, *Numeri idonei*.

Comme nous l'avons vu au paragraphe précédent, il est superflu de considérer toutes les formes réduites pour chacun de ces déterminants ; il suffit de savoir qu'il n'y a qu'une seule classe par genre. Dès lors, on a cet énoncé remarquable, Δ étant une des soixante-cinq valeurs énumérées plus haut.

« Tout nombre premier dont $-\Delta$ est résidu, peut être mis sous la forme $x^2 + \Delta y^2$ d'une seule façon ».

On peut aussi dire : tout nombre dont $-\Delta$ est résidu et qui ne peut pas être mis sous la forme $x^2 + \Delta y^2$ est composé (des facteurs dont $-\Delta$, est non-résidu pour un nombre pair de ces facteurs). Ou encore, si le nombre N peut être mis sous la forme $x^2 + \Delta y^2$, il est premier si la solution $x^2 + \Delta y^2 = \mathrm{N}$ est unique. Ce nombre est composé, si on parvient à trouver une deuxième solution de $x^2 + \Delta y^2 = \mathrm{N}$.

Ainsi, non seulement, il est superflu de considérer les formes trinomes, mais parmi les formes binomes, on peut encore choisir une seule, par exemple, la forme $f = x^2 + \Delta y^2$ qui a l'avantage de donner un caractère, le plus simple du genre, $\left(\frac{f}{p}\right) = +1$, pour tout facteur impair p de Δ.

TROISIÈME PARTIE.

Factorisation.

CHAPITRE X.

Les résidus quadratiques.

1. La théorie des résidus quadratiques étant d'une importance capitale dans les questions de factorisation, nous croyons devoir en rappeler les principales conclusions, en renvoyant pour les détails, à la Première Partie de notre ouvrage (T, I, p. 59 et suivantes).

Définition. — Étant donné un nombre premier $p \geqslant 3$ et un nombre quelconque $q \neq 0$, on dira que q est *résidu quadratique* de p, quand on peut trouver un nombre x tel que $x^2 \equiv q$ (Mod. p).

On écrira $\left(\frac{q}{p}\right) = +1$ pour exprimer que q est un résidu quadratique de p.

Si la congruence $x^2 \equiv q$ (Mod. p) n'est pas possible, on dira que q est un *non-résidu quadratique* de p.

Quand il n'y aura aucune confusion à craindre, nous dirons simplement que q est résidu ou non résidu de p suivant que la congruence $x^2 \equiv q$ (Mod. p) est possible ou non.

On écrira $\left(\frac{q}{p}\right) = +1$, ou $\left(\frac{q}{p}\right) = -1$, suivant que q est ou n'est pas résidu de p.

On sait que la congruence $x^2 \equiv q$ (Mod. p) est possible ou non suivant qu'on aura

$$q^{\frac{p-1}{2}} \equiv +1, \qquad \text{ou} \qquad -1 \ (\text{Mod. } p).$$

Il en résulte qu'on aura

$$\left(\frac{q}{p}\right) = q^{\frac{p-1}{2}}.$$

Telle est une autre définition du *symbole de* LEGENDRE $\left(\frac{q}{p}\right)$.

2. THÉORÈMES SUR LES RÉSIDUS.

1° $$\left(\frac{1}{p}\right) = 1, \qquad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

En d'autres termes, 1 est toujours un résidu, (-1) est résidu des nombres premiers de la forme $4k+1$, et non résidu des nombres de la forme $4k+3$ (T, IV, p. 6).

2° Si $$q = q_1 q_2 q_2 \cdots$$

$$\left(\frac{q}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\left(\frac{q_3}{p}\right), \quad \cdots$$

Il en résulte que tout carré parfait est résidu

$$\left(\frac{a^2}{p}\right) = \left[\left(\frac{a}{p}\right)\right]^2 = \left[\pm 1\right]^2 = +1.$$

Il suit encore de là, qu'on peut négliger dans q, tout facteur carré. Si, par exemple

$$q = a^2 q', \qquad \left(\frac{q}{p}\right) = \left(\frac{q'}{p}\right).$$

3° Si p est de la forme $4k+1$, les nombres q et $-q$ sont tous les deux résidus, ou tous les deux non résidus

$$\left(\frac{q}{p}\right) = \left(\frac{-q}{p}\right).$$

Mais, si p est de la forme $4k+3$, les nombres q et $-q$ sont : l'un résidu, l'autre non résidu

$$\left(\frac{q}{p}\right) = -\left(\frac{-q}{p}\right).$$

4° Si $$q \equiv q' \text{ (Mod. } p), \qquad \left(\frac{q}{p}\right) = \left(\frac{q'}{p}\right).$$

5° Le produit de deux résidus, ou de deux non résidus, est un résidu. Le produit d'un résidu par un non résidu, est un non résidu.

6° 2 est résidu des nombres premiers de la forme $8k \pm 1$, et non résidu des nombres premiers de la forme $8k \pm 3$.

— 2 est résidu des nombres premiers de la forme $8k + 1$, ou $8k + 3$, et non résidu des nombres premiers de la forme $8k + 5$, ou $8k + 7$.

7° Si q est premier $\geqslant 3$.

On aura

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

En d'autres termes, les symboles $\left(\frac{q}{p}\right)$ et $\left(\frac{p}{q}\right)$ ont la même valeur, si un des nombres q ou p est de la forme $4k + 1$. Ces symboles diffèrent, si les deux nombres p et q sont de la forme $4k + 3$.

3. On a supposé que $q \neq 0$. Si $q \equiv 0$ (Mod. p), la congruence $x^2 \equiv 0$ (Mod. p), est évidemment possible et admet la solution $x \equiv 0$ (Mod. p).

Mais $x \equiv 0$ (Mod. p) donne $x^2 \equiv 0$ (Mod. p^2).

Il en résulte que $q \equiv 0$ (Mod. p) n'est résidu que si on a $q \equiv 0$ (Mod. p^2).

En raison de cette particularité du résidu 0, nous dirons que 0 est *semi-résidu*.

4. Résidus d'un nombre composé.

Supposons maintenant que p soit composé, $p = p_1, p_2, p_3, \ldots$. Si la congruence $x^2 \equiv q$ (Mod. p) est possible, les congruences

$$x^2 \equiv q \text{ (Mod. } p_1),$$

$$x^2 \equiv q \text{ (Mod. } p_2),$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

le seront aussi.

Ainsi, *si q est résidu d'un nombre composé p, le nombre q est aussi résidu de tout facteur de p.*

Inversement, si q est résidu des nombres $p_1, p_2, p_3, \ldots$, le nombre q est résidu de leur produit $p = p_1 p_2 p_3, \ldots$.

5. Symbole de Jacobi.

Posons $p = p_1 p_2 p_3, \ldots,$ et par définition

$$\left(\frac{q}{p}\right) = \left(\frac{q}{p_1}\right)\left(\frac{q}{p_2}\right)\left(\frac{q}{p_3}\right), \quad \ldots.$$

$\left(\frac{q}{p}\right)$ sera dit *symbole de* Jacobi, si p est composé.

6. Il y a lieu de remarquer qu'il y a une différence essentielle entre le symbole de Legendre $\left(\frac{q}{p}\right)$ et celui de Jacobi.

Si p est premier, le symbole de Jacobi ne diffère pas de celui de Legendre. Mais, si p est composé, il se peut que chacun des symboles

$$\left(\frac{q}{p_1}\right), \quad \left(\frac{q}{p_2}\right), \quad \left(\frac{q}{p_3}\right), \quad \ldots,$$

ait une valeur $+1$, alors $\left(\frac{q}{p}\right) = +1$, et q est un résidu de $p = p_1 p_2 p_3, \ldots,$ c'est-à-dire, la congruence $x^2 \equiv q$ (Mod. p), est possible.

Il peut aussi arriver que q soit un non résidu d'un nombre impair de facteur p_i, alors $\left(\frac{q}{p}\right) = -1$, et q n'est pas résidu, et la congruence $x^2 \equiv q$ (Mod. p), n'est pas possible.

Mais, il peut aussi arriver que q, soit un non résidu d'un nombre pair de facteurs p_i, alors $\left(\frac{q}{p}\right) = +1$, et cependant la congruence $x^2 \equiv q$ (Mod. p), n'est pas possible.

Nous dirons dans ce cas que le nombre q est résidu de Jacobi, mais un non résidu de Legendre.

Remarquons que tout résidu de Legendre, est résidu de Jacobi, mais un résidu de Jacobi, n'est pas résidu de Legendre, que dans le cas ou il est résidu de chaque facteur de p.

7. Si un nombre N (premier ou composé), peut être mis sous la forme $N = x^2 \pm Dy^2$, le nombre $(\mp D)$ est résidu de N (T, IV, p. 35).

C'est là un moyen puissant de trouver des résidus d'un nombre dont on ignore la nature (premier ou composé).

8. Problème. — Déterminer des résidus d'un nombre dont on ignore la nature.

On trouvera une série de formes quadratiques $N = x^2 \pm D_i\, y^2$, avec différentes valeurs de x et y.

Les résidus $\mp D_i$ seront combinés entre eux pour donner par leur produit des résidus plus simples. Si ces formes sont suffisamment nombreuses, on trouvera plusieurs résidus du nombre N.

9. Théorème. — Si $N = x^2 \pm R$, le nombre R n'est divisible que par des nombres p, tel que $\left(\frac{N}{p}\right) = +1$.

En effet, si R est divisible par p, l'égalité $N = x^2 \pm R$, devient $N \equiv x^2$ (Mod. p), d'où $\left(\frac{N}{p}\right) = 1$.

Ainsi, si $\left(\frac{N}{p}\right) = -1$, le nombre p n'entrera jamais comme facteur dans $\pm (x^2 - N)$.

Toutefois, on peut mettre en évidence, les facteurs p tel que $\left(\frac{N}{p}\right) = -1$, en mettant N sous la forme $N = kx^2 + R$, k étant lui-même un non résidu de p.

10. Pour mettre un nombre donné N sous la forme $N = x^2 \pm Dy^2$, on n'a qu'à diviser $R = \mp (x^2 - N)$ par le plus grand carré possible. Si R n'est divisible par aucun carré, on prendra $y = 1$.

Bien que le nombre des formes $N = x^2 \pm Dy^2$ soit illimité, très peu de ces formes sont utilisables.

D'ailleurs, si on prend pour x une valeur arbitraire, la différence $\mp (x^2 - N)$ n'est divisible par aucun carré. En général, on aura assez difficile de factoriser R, si x est arbitraire et N quelque peu grand.

Il en est tout autrement, si on procède avec méthode, de la façon que nous indiquerons dans les numéros qui suivent.

11. Le premier soin sera de déterminer les petits nombres r_i pour lesquels N est résidu. Soit

$$r_1, r_2, r_3, r_4, \ldots.$$

les nombres r_i tels que $\left(\frac{N}{r_i}\right) = +1$.

On n'utilisera ce procédé que si beaucoup de petits résidus 3, 5, 7, 11, 13, 17, 19, ..., figurent parmi les r_i.

Toutefois, seuls les petits nombres (disons les nombres premiers inférieurs à 50), seront vérifiés directement, l'application de la méthode que nous exposons, fera connaître, sinon tous les autres (il y en a une infinité), du moins plusieurs des autres.

12. On déterminera x de telle sorte que la différence $\mp(x^2 - N)$, soit divisible par

$$r_1,\ r_1^2,\ r_1^3,\ \ldots,\ r_1^k,$$

$$r_2,\ r_2^2,\ r_2^3,\ \ldots,\ r_2^e,$$

$$r_3^2,\ r_4^2,\ r_5^2,\ \ldots,$$

$$r_3^2 r_4^2,\ r_3^2 r_5^2 \ldots,$$

$$r_3^2 r_4^2 r_5^2 \ldots.$$

On prendra chaque fois x aussi voisin que possible de $\sqrt{N}$.

Puisqu'on connait d'avance certains diviseurs de R, on n'aura pas de difficultés pour mettre R sous la forme Dy^2, le nombre D n'étant divisible par aucun carré.

Les facteurs qu'on rencontre dans les différentes valeurs de D seront subdivisés en trois catégories :

1° Petits facteurs dans le genre de r_i qui n'ont pas été envisagés.

2° Facteurs voisins de $\sqrt[4]{N}$.

3° Les grands facteurs.

Les facteurs de la première catégorie seront utilisés comme les r_i.

Ceux de la deuxième catégorie, le seront en cherchant la valeur de x voisine de $\sqrt{N}$ et telle que $\mp (x^2 - N)$ soit divisible par le carré de ce facteur.

Les facteurs de la troisième catégorie peuvent encore être quelquefois utilisés, mais on cherchera à rendre R divisible par ce facteur, sans chercher à faire intervenir le carré de ce facteur.

Exemple 1.

$$N = 535 \times 2^{30} + 1.$$

On trouve

$$N = 1054929^2 - 2.2909.9620^2.$$

Il en résulte que le nombre 2.2909 est résidu de N. Ce résidu est peu commode. On trouvera encore

$$N = 327679^2 + 2.2909.8960^2,$$

d'où le résidu -2.2909.

Les nombres (2.2909) et (-2.2909) étant résidus, le produit -5818^2 l'est aussi, d'où le résidu très commode -1.

On trouve encore

$$N = 718721^2 + 41.353.2000^2,$$

$$714485^2 + 2.13.37.353.434^2,$$

$$757671^2 + 13.37.41.140^2,$$

d'où les résidus

$$(-41.353), \qquad (-2.13.37.353), \qquad (-13.37.41),$$

dont le produit se réduit à -2 après l'élimination du carré de (41.353.13.37).

Exemple 2.

$$N = 1 + 219 \times 2^{29} = 117574729729.$$

On trouve

$$\left.\begin{aligned} (\text{Mod. } N) \quad 343039^2 &\equiv 2^{11} \times 3^5 \times 7 \times 29, \\ 342869 &\equiv -8.3^4.29.829, \\ 364423^2 &\equiv 16.3^8.5^2.7.829, \end{aligned}\right\} \quad (1)$$

$$\left.\begin{aligned} 260576^2 &\equiv -1637^2 \times 3 \times 37 \times 167, \\ 309173 &\equiv -8 \times 5^2 \times 3^7 \times 7 \times 43 \times 167, \\ 346927^2 &\equiv 2^5 \times 3^7 \times 5^2 \times 37 \times 43, \end{aligned}\right\} \quad (2)$$

$$\left.\begin{aligned} 342707^2 &\equiv -8 \times 5 \times 3^6 \times 43 \times 101, \\ 147171^2 &\equiv -677^2 \times 8 \times 7 \times 37 \times 101, \\ 346927^2 &\equiv 2^5 \times 3^7 \times 5^2 \times 37 \times 43, \end{aligned}\right\} \quad (3)$$

$$\left.\begin{aligned} 84283^2 &\equiv -661^2 \times 8 \times 5 \times 3 \times 7^2 \times 43, \\ 230073^2 &\equiv -587^2 \times 16 \times 5^2 \times 7 \times 67, \\ 344777^2 &\equiv 16 \times 5^5 \times 9 \times 43 \times 67. \end{aligned}\right\} \quad (4)$$

(1) donne les résidus 2.3.7.29, $-2.29.829$ et 7.829, dont le produit est $-3a^2$. On aura ainsi le résidu -3.

(2) donne les résidus $-3.37.167$, $-2.3.7.43.167$ et 2.3.37.43 dont le produit est $3.7b^2$, d'où le résidu 3.7 et puisque -3 est résidu, -7 est aussi résidu.

(3) donne de même, le résidu 2.3.5.7 et puisque 3×7 est résidu, on aura le résidu 2×5.

Enfin (4), donne les résidus, $-2.5.3.43$, -7×67 et $5 \times 43 \times 67$, dont le produit se réduit à $2.3.7c^2$, d'où le résidu 2.3.7 et puisque 3×7 est résidu, 2 est aussi résidu. D'autre part, 2×5 et 2 étant résidu, 5 est aussi résidu.

On aura ainsi les résidus $+2$, -3, $+5$, -7.

13. Dans certains cas, on peut déterminer un résidu $\mp$ D par la résolution directe de l'équation $N = x^2 \pm Dy^2$.

Soit, pour fixer les idées $N = 4k + 1$, alors -1 peut être résidu de N. Pour être fixé à ce sujet, il suffit de résoudre l'équation $x^2 + y^2 = N$. Si on y arrive, le nombre -1 est effectivement résidu. Si on est certain que l'équation $N = x^2 + y^2$ n'est pas possible, le nombre -1 n'est pas résidu. Le nombre N est alors composé.

Il est toutefois difficile de vérifier l'impossibilité de l'équation $x^2 + y^2 = N$, si N est quelque peu grand.

On se servira alors des formes $x^2 \pm D_i\, y^2$.

Si ces formes sont judicieusement choisies et suffisamment nombreuses, on peut arriver à isoler n'importe quel résidu de N.

Si, par conséquent, certaines valeurs de p_i ne peuvent être isolées, il y a lieu de supposer que ces valeurs sont des non résidus de N et N doit être composé.

Toutefois, on n'a de preuves certaines, qu'un nombre donné p_i est un non résidu de N, que si on parvient à établir l'impossibilité de la congruence $x^2 \equiv p_i$ (Mod. N), ce qui est parfois possible.

On aura ainsi un *renseignement négatif* sur le nombre N, qu'on mettra à profit pour la recherche des facteurs de N.

Ainsi, p_1, p_2, p_3, ..., désignant des nombres pour lesquels $\left(\frac{N}{p_i}\right) = +1$, on tâchera de subdiviser ces nombres en deux catégories :

1° Nombres qui sont résidus de N.

2° Nombres qui ne sont pas résidus de N.

Les renseignements de la première catégorie sont plus précieux et peuvent toujours être utilisés. Les renseignements négatifs (de la deuxième catégorie) ne peuvent l'être que sous certaines réserves, en particulier, quand N ne contient que deux facteurs.

14. Dans bien des cas, il est utile de s'assurer que le nombre à factoriser ne contient pas plus de deux facteurs.

Soit pour fixer les idées, le nombre impair N, qui est de la forme $8k + 1$, 3, 5 ou 7.

Si $N \equiv 1$ (Mod. 8), et si N ne contient pas plus de deux facteurs, ces deux facteurs seront $\equiv 1 \times 1$, 3×3, 5×5 ou 7×7 (Mod. 8). Si les facteurs sont $\equiv 1 \times 1$, les trois nombres -1 et ± 2 sont résidus de chaque facteur, donc de N ; si $N \equiv 3 \times 3$ (Mod 8), le nombre -2 seul est résidu N. Le nombre -1 seul est résidu de N, si $N \equiv 5 \times 5$, enfin si $N \equiv 7 \times 7$, le nombre $+2$ seul est résidu.

Ainsi, si le nombre N est de la forme $8k + 1$ et si N ne contient pas plus de deux facteurs, l'une au moins des représentations

$$N = x^2 + y^2, \qquad N = x^2 + 2y^2, \qquad N = x^2 - 2y^2,$$

est possible.

Mais on ne peut rien affirmer, si N peut contenir plus de deux facteurs ; par exemple, on peut avoir

$$N \equiv 3 \times 5 \times 7 \text{ (Mod. 8)},$$

et aucun des nombres -1, ± 2, n'est résidu de N, bien que ces trois nombres soient résidus jacobiens.

Si $N \equiv 3$ (Mod. 8), on aura dans le cas de deux facteurs

$$N \equiv 1 \times 3 \quad \text{ou} \quad 5 \times 7.$$

Dans le premier cas, -2 est résidu de N, dans le deuxième cas non résidu.

Si $N \equiv 5$, on aura $N \equiv 1 \times 5$ ou 3×7.

Dans le premier cas, -1 est résidu, dans le deuxième cas non résidu de N.

Enfin, si $N \equiv 7$ (Mod. 8), on aura $N \equiv 1 \times 7$ ou 3×5 et 2 est résidu de N dans le premier cas et non résidu dans le deuxième cas.

Inversement, si N contient deux facteurs, et si N est de la forme $8k + 1$, les deux facteurs seront

$$1 \times 1, \quad 3 \times 3, \quad 5 \times 5 \quad \text{ou} \quad 7 \times 7,$$

suivant que les nombres 1 et ± 2 seront

-1	Résidu,	Non résidu,	Résidu	Non résidu.
$+2$	Résidu,	Non résidu,	Non résidu,	Résidu.
-2	Résidu,	Résidu,	Non résidu,	Non résidu.

Si $N \equiv 3$, les deux facteurs seront

$$1 \times 3, \quad 5 \times 7,$$

suivant que le nombre -2 sera

Résidu, ou non résidu de N.

Si $N \equiv 5$, les deux facteurs seront

$$1 \times 5, \quad \text{ou} \quad 3 \times 7,$$

suivant que le nombre -1 sera

Résidu, ou non résidu de N.

Enfin, si $N \equiv 7$, les deux facteurs seront

$$1 \times 1, \qquad 3 \times 5,$$

suivant que le nombre 2 sera

Résidu, ou non résidu de N.

On remarquera que le cas de $N \equiv 1$ (Mod. 8), se comporte bien autrement que les autres cas $N \equiv 3$, 5 ou 7.

En effet, si N ne contient pas plus de deux facteurs, le nombre N admettra au moins un résidu parmis les nombres -1, ± 2.

Enfin, signalons qu'il suit de ce qui précède, que si $N \equiv 1$ (Mod. 8), et si aucun des nombres 1, ± 2 n'est résidu de N, le nombre N est composé d'au moins trois facteurs.

On aura, en résumé, les théorèmes suivants :

1° *Tout nombre de la forme* $8k + 1$ *qui contient au plus deux facteurs. peut être mis sous l'une des trois formes* $x^2 + y^2$, $x^2 + 2y^2$, $x^2 - 2y^2$.

2° *Tout nombre impair qui ne peut être mis sous aucune des trois formes* $x^2 + y^2$, $x^2 + 2y^2$, $x^2 - 2y^2$ *est composé. Si ce nombre est de la forme* $8k + 1$, *il contient au moins trois facteurs.*

15. Pour s'assurer que N ne contient pas plus de deux facteurs, il suffit d'examiner tous les facteurs possibles de N (compatibles avec les formes quadratiques obtenues par les différents résidus) inférieurs à $\sqrt[3]{N}$.

En effet, si N contient plus de deux facteurs, le plus petit facteur sera $\leqslant \sqrt[3]{N}$.

Cette constatation est utile à plusieurs points de vue. D'abord, les petits facteurs se rencontrent bien plus souvent que les grands facteurs, et il serait déraisonnable de s'exposer à un travail souvent fastidieux pour trouver, en fin de compte, que le nombre N est divisible par un petit facteur.

Ainsi $\frac{1}{3}$ de tous les nombres est divisible par 3.

Environ 0.9 de tous les nombres ont un facteur inférieur à 100.

En moyenne, $\frac{14}{15}$ de tous les nombres, ont un facteur inférieur à 1000, $\frac{19}{20}$ de tous les nombres, ont un facteur inférieur à 10000, etc.

Enfin, si on est amené à la décomposition de N par l'équation $N = x^2 - y^2$, les limites de x seront d'autant plus rapprochées que la limite du plus petit facteur sera plus élevée.

CHAPITRE XI.

Preuves directes de primalité.

1. Dans certains cas, on peut prouver qu'un nombre donné est premier, sans essayer les diviseurs éventuels de ce nombre.

On conçoit facilement l'avantage d'une telle preuve, quand elle est possible. S'il s'agit d'un nombre suffisamment grand, les calculs exigés par la preuve, sont sensiblement plus simples que ceux demandés par la décomposition de ce nombre. Et si on arrive à démontrer que le nombre considéré est premier, on aura évité les calculs inutiles faits pour essayer de le décomposer. Mais, par contre, si la preuve ne réussit pas (et, en particulier, si le nombre considéré est composé), les calculs effectués pour la preuve de la primalité, constituent une pure perte, sauf peut être qu'ils donnent parfois la certitude que le nombre considéré est composé. Encore, dans ce cas, on n'est pas avancé pour la décomposition effective du nombre considéré.

2. D'après le théorème de Fermat, on a

$$a^{N-1} \equiv 1 \text{ (Mod. N)}, \tag{1}$$

si N est premier et a non divisible par N.

Cette relation peut aussi avoir lieu si N est composé. Soit $N \equiv n'n''n'''$, ..., et soit m le plus petit multiple de $\varphi(n')$, $\varphi(n'')$, $\varphi(n''')$, ... [1]. On aura alors, quel que soit x premier avec N, $x^m \equiv 1$ (Mod. N).

Si on désigne par d le plus grand commun diviseur de $N-1$ et m, on aura $m = kd$, $N - 1 = ld$.

Posons $$a \equiv x^k \text{ (Mod. N)},$$
et on aura
$$x^m \equiv x^{kd} \equiv a^d \equiv 1 \text{ (Mod. N)},$$
ce qui entraîne
$$a^{ld} \equiv 1, \qquad \text{ou} \qquad a^{N-1} \equiv 1 \text{ (Mod. N)}.$$

Ainsi la réciproque du théorème de Fermat, doit s'énoncer comme suit :

Si la congruence $a^x \equiv 1$ (*Mod.* N), *a lieu pour* $x = N - 1$, *sans l'être quand* x *est sous-multiple de* $N - 1$, *le nombre* N *est premier.*

---

(1) n', n'', ..., sont supposé premiers entre eux ; $\varphi(n)$ est l'indicateur de n (T, I, p. 10).

Ou encore :

Si la **plus petite** *solution de la congruence* $a^x \equiv 1$ (*Mod.* N) *est* $x = N - 1$, *le nombre* N *est premier.*

3. On peut énoncer autrement la réciproque du théorème de Fermat :

Si la congruence $a^{N-1} \equiv 1$ (*Mod.* N) *n'est pas satisfaite, le nombre* N *est composé.*

Exemple. Soit le nombre

$$N = 1 + 369 \times 2^{19}.$$

On trouve que la relation

$$2^{N-1} \equiv 1 \text{ (Mod. N)},$$

n'est pas vérifiée. Il en résulte que N est composé.

Mais en effectuant le calcul de 2^{N-1}, on trouve

$$241.2^{15} \equiv 2256, \qquad \text{ou} \qquad 2256.9.583 \equiv 1,$$

ce qui conduit aux facteurs

$$N = 6337 \times 30529.$$

4. Les deux énoncés de la réciproque du théorème de Fermat, ont leurs avantages et leurs inconvénients.

Le premier énoncé est trop restrictif. Ainsi le nombre N est premier, si la plus petite valeur de x pour laquelle la relation $a^x \equiv 1$ (Mod. N) a lieu est [1]

$$x = \frac{N - 1}{k} \; (k \leqslant 12).$$

Le nombre N peut aussi être premier quand $k > 5$, mais il parait difficile de l'établir par la réciproque du théorème de Fermat.

Soit, par exemple

$$N = 2^{61} - 1.$$

Seelhof (1886) a établi que

$$3^{\frac{N-1}{2}} \equiv -1 \text{ (Mod. N)}.$$

Or

$$\frac{N - 1}{2} = 2^{60} - 1 = 3^2.5^2.7.11.13.31.41.61.151.331.1321.$$

---

[1] Pomey. Comptes Rendus, 1924, p. 987-990.

Seelhof en a conclu que $N = 2^{61} - 1$ est premier.

La démonstration de Seelhof est insuffisante. En réalité, pour avoir la certitude que N est premier, il faut établir que non seulement

$$3^{\frac{N-1}{2}} \equiv -1 \text{ (Mod. N)},$$

mais encore que la congruence

$$3^{\frac{N-1}{2k}} \equiv -1 \text{ (Mod. N)},$$

n'a pas lieu pour

$$k = 3, 5, 7, 11, 13, 31, 41, 61, 151. 331, 1321.$$

Et encore, si la congruence

$$3^{\frac{N-1}{2k}} \equiv -1 \text{ (Mod. N)},$$

avait lieu pour une de ces valeurs de k, en résultera-t-il que N est composé ?

Nullement, seulement il manquera la certitude que N est premier.

En réalité, bien que la démonstration de Seelhof, soit insuffisante, N est premier, comme il a été établi par d'autres procédés.

Le deuxième énoncé de la réciproque du théorème de Fermat, a l'avantage de préciser dans certains cas, la nature du nombre N.

Ainsi, en 1878, Lucas établit $F_6 = 2^{64} + 1$, est composé, ce n'est qu'en 1880 que Landry est parvenu à décomposer, ce nombre.

En 1909, Morehead et Western, ont établi que $F_7 = 2^{128} + 1$ et $F_8 = 2^{256} + 1$, sont composés. Mais on ne connaît pas les facteurs de ces nombres.

5. On remarquera encore que le deuxième énoncé n'exige pas qu'on connaisse la décomposition de $N - 1$, tandis que le premier énoncé suppose qu'on connaît la décomposition de $N - 1$.

Nous ajouterons que pratiquement le premier énoncé n'est utile que si $N - 1$ n'admet pas beaucoup de facteurs impairs différents.

Il en est en particulier ainsi, pour $N = \lambda.2^n + 1$, si λ n'est pas très grand. Alors, il devient possible de s'assurer si la congruence $a^x \equiv 1$ (Mod. N), a, ou n'a pas lieu pour $x = \frac{N-1}{k}$.

6. Il résulte de ce qui précède, que par la résolution de la congruence $a^x \equiv 1$ (Mod. N), on a une preuve directe de la primalité de N.

Nous avons résolu cette congruence pour les cas particuliers suivants :

1° $a = 10$, $3 < N \leqslant 27457$ (1),

2° $a = 2$, $3 < N < 300000$ (2).

3° $a = 2$, $1 < N = 2^x 3^y 5^z + 1 < 10^7$ (3),

4° $a = 2$, $1 < N = 512k + 1 < 10^7$ (4).

5° $a = 3$, $1 < N < 10^3$ (5).

6° $a = 5$, $1 < N < 10^3$ (6).

7° $a = 2$, $10^8 < N = k.2^n + 1 < 10^{12}$, $1 \leqslant k \leqslant 999$ (7).

L'importance de la question, nous engage à nous y arrêter pour signaler certains procédés propres à faciliter le travail, qui parfois est fastidieux.

7. Considérons d'abord le cas ou $N - 1$ ne contient qu'un seul diviseur impair, on aura $N - 1 = k.2^n$, k étant premier.

Il y a lieu de distinguer deux cas, suivant qu'on connaît la nature du nombre N ou non.

1° Quand on sait que nombre N est premier, on aura simplement à vérifier si le nombre a est résidu $k^{ième}$, quadratique, biquadratique, etc.

2° Si on ne connaît pas la nature du nombre N, on calculera la valeur $a^{2^{n-1}} \equiv y$ (Mod. N) et $y^k \equiv z$ (Mod. N).

---

(1) Recherches sur la Théorie des Nombres, Paris, Gauthier-Villars, p. 131-145.
(2) » » » » p. 131-191.
(3) » » » » p. 53.
(4) » » » » p 192-204.
(5) » » » » p. 65.
(6) » » » » p. 65.
(7) » » » » p. 53.
Voir aussi le dernier chapitre de cet ouvrage.

Le nombre N est premier si $z \equiv \left(\frac{a}{N}\right)$.

Toutefois, dans certains cas, il est avantageux d'éviter le calcul de y^k, en particulier, si $k = l.2^a - 1$.

Ainsi, si $k = 7$, on calculera les nombres (Mod. N) y, y^2, y^4, et y^8. Si le nombre N est premier, on aura $y^8 \equiv \pm y$.

De même, si $k_1 = 31$, on calculera les nombres y, y^2, y^4, y^8, y^{16}, y^{32} et on aura $y^{32} \equiv \pm y$, si le nombre N est premier.

Soit encore $k = 23$.

On calculera les nombres

$$y, \quad y^2, \quad y^4, \quad y^8, \quad y^{16}, \quad y^{24} \equiv y^8 \times y^{16}.$$

On aura $y^{24} \equiv y$, si le nombre N est premier.

8. Un cas particulier qui mérite d'être signalé est celui de $k = 3$.

D'une façon générale, si 3 entre comme facteur de $N - 1$, on peut abréger le calcul comme suit.

Posons $$N - 1 = 3m.$$

Puisque $$a^{N-1} \equiv a^{3m} \equiv 1,$$

on aura $$a^{2m} + a^m + 1 \equiv 0.$$

Ainsi, on calculera

$$a^m \equiv z \quad \text{et} \quad z^2 \equiv -z - 1,$$

si N est premier. Naturellement, si a est un résidu cubique de N, on aura simplement $a^k \equiv 1$.

Si, d'une façon générale, on trouve

$$a^n \equiv b, \quad b^2 \equiv b - 1,$$

on en tirera

$$b^2 - b + 1 \equiv 0, \quad \text{ou} \quad b^3 \equiv -1, \quad \text{ou} \quad a^{3n} \equiv -1,$$

ou enfin $$a^{6n} \equiv 1.$$

9. Considérons ensuite le cas où $N - 1$ contient deux facteurs impairs

$$N = 1 + kl.2^n.$$

Quand on sait que N est premier, on vérifiera si le nombre a est un résidu d'ordre 2^λ, k, l, $(\lambda \leqslant n)$.

Si on ne sait rien sur le nombre N, on calculera le nombre

$$a^{2^n-1} \equiv y, \qquad y^a \equiv z, \qquad y^b \equiv u, \qquad z^b \equiv u^a \equiv v.$$

Le nombre N est premier, si

$$v \equiv \left(\frac{a}{\mathrm{N}}\right).$$

En pratique, on trouvera plusieurs fois l'occasion d'abréger le calcul. Ainsi, si $kl = 3 \times 5$, on calculera

$$y, \qquad y^2, \qquad y^4, \qquad y^5, \qquad \text{et} \qquad y^{10},$$

et on sera fixé sur le résultat.

Si $y^2 \equiv y - 1$, on aura $y^3 \equiv -1$, ou $a^{\frac{\mathrm{N}-1}{5}} \equiv 1$,

$y^5 \equiv -1$, $\qquad a^{\frac{\mathrm{N}-1}{3}} \equiv 1$,

$y^{10} \equiv y^5 - 1$, $\qquad a^{\mathrm{N}-1} \equiv 1$.

10. Si N — 1, contient trois facteurs impairs, soit

$$\mathrm{N} = 1 + klm2^n.$$

On aura encore à considérer les deux cas.

1° On sait que N est premier. Alors, résoudre la congruence $a^x \equiv 1$ (Mod. N), revient à déterminer si a est un résidu d'ordre

$$2^\lambda\ (\lambda \leqslant n),\ k,\ l,\ m,$$

ou d'une façon générale d'ordre i, i étant un sous-multiple de N — 1.

2° On ne sait rien sur la nature de N.

On déterminera alors $a^{2^n-1} \equiv y$ (Mod. N) et on calculera (Mod. N)

$$y^k \equiv u, \qquad u^l \equiv v, \qquad v^m = \left(\frac{a}{\mathrm{N}}\right).$$

On déterminera, si la congrnence $a^x \equiv 1$, a lieu pour une valeur de x égale à un sous-multiple de la solution trouvée.

11. Les séries de LUCAS, ont l'avantage sur la réciproque du théorème de FERMAT, d'être applicables aussi bien quand on connaît la décomposition de N + 1, que lorsque l'on connaît celle de N — 1.

Voici, en résumé, leur application :

Étant donné l'équation $x^2 - px - q = 0$, p et q étant des entiers, soient a et b les racines de cette équation (rationnelles ou irrationnelles, réelles ou imaginaires).

Posons

$$u_n = \frac{a^n - b^n}{a - b}, \qquad v_n = a^n + b^n.$$

On aura

$$u_{n+1} = pu_n + qu_{n-1}, \qquad v_{n+1} = pv_n + qv_{n-1}.$$

On aura encore

$$u_{2n} = u_n v_n, \qquad v_{2n} = v_n^2 - 2q^n,$$

$$\Delta = d^2 = (a - b)^2 = p^2 - 4q.$$

$u_n \equiv 1$, $\quad u_{n-1} \equiv 0$, si n est premier et $\left(\frac{\Delta}{n}\right) = +1$.

$u_n \equiv -1$, $\quad u_{n+1} \equiv 0$, $\qquad \left(\frac{\Delta}{n}\right) = -1$,

En pratique, on prendra

$$q = \pm 1, \qquad \text{alors} \qquad v_{2n} = v_n^2 \pm 2.$$

Soit maintenant un nombre

$$N = k.2^n + 1, \qquad N - 1 = k.2^n.$$

On utilisera une série telle

$$\left(\frac{\Delta}{n}\right) = +1.$$

Par exemple, la série provenant de l'équation

$$x^2 - 3x + 2 = 0.$$

On aura

$$u_{N-1} \equiv 0, \qquad \text{ou} \qquad 2k.2^n \equiv 1,$$

ce qui est la réciproque du thèorème de FERMAT.

En particulier, pour $N = 2^{2k} + 1$, on vérifiera la congruence

$$3^{\frac{N-1}{2}} \equiv -1,$$

puisque $\left(\frac{3}{N}\right) = -1$.

On peut aussi avec Lucas, considérer la série provenant de l'équation $x^2 - 2x - 1 = 0$, donnant $\Delta = 8$.

Si on a à étudier un nombre de la forme $k.2^n - 1$, on prendra une série telle que $\left(\frac{\Delta}{N}\right) = -1$.

En particulier, pour les nombres de la forme $2^n - 1$, on prendra des séries provenant des équations

$$x^2 - x - 1 = 0, \qquad \text{ou} \qquad x^2 - 4x + 1 = 0.$$

12. Considérons un nombre de la forme $N = 2^k + 1$.

Un tel nombre ne peut être premier que si l'exposant est une puissance de 2, car si l'exposant contient un facteur impair $k = l.m$, $N = 2^{lm} + 1$, sera divisible par $2^l + 1$ et par $2^m + 1$. On aura donc $k = 2^n$.

Soit donc un nombre $F_n = N = 2^{2^n} + 1$.

Ce nombre est premier si $3^{\frac{N-1}{2}} \equiv -1$.

On peut aussi étudier le nombre F_n par la considération de la série provenant de l'équation

$$x^2 - 2x - 1 = 0, \qquad \Delta = 8.$$

$$\left(\frac{\Delta}{n}\right) = +1, \qquad u_{N-1} \equiv 0.$$

On aura ainsi $\qquad u_{2^{2^n}} \equiv 0.$

Or

$$u_{2k} = u_k v_k, \qquad v_{2k} = v_k - 2(-1)^k.$$

On aura ainsi

$$u_{2^{2^n}} \equiv v_{2^{2^n}-1}.v_{2^{2^n}-2}.v_{2^{2^n}-3}. \ldots v_4 v_2 v_1 u_1.$$

Or

$$u_1 = 1, \quad v_1 = 2, \quad v_2 = 6, \quad v_4 = v^2 - 2 = 34, \quad v_8 = v_4^2 - 2, \ldots$$

Puisque ce produit est nul, l'un des v est nul.

Ainsi, dans la série

$$v_1 = 2, \quad v_2 = 6, \quad v_4 = v^2 - 2, \quad v_8 = v_4^2 - 2, \quad \ldots \quad (1)$$

ou par un changement de numérotage, la série

$$v_1 = 2, \; v_2 = 6, \; v_3 = v_2^2 - 2, \; v_4 = v_3^2 - 2, \; \ldots, \; v_i^2 = v_{i-1}^2 - 2, \; (2)$$

finit par un terme nul.

L'ordre de ce terme est au plus 2^{2^n-1} dans (1) ou 2^n dans (2).

13. Considérons ensuite un nombre $M = 2^n - 1$. Ce nombre ne peut être premier que si n l'est, car si n n'est pas premier, soit $n = ab$ et $2^n - 1$ est divisible par $2^a - 1$ et $2^b - 1$.

Supposons donc que n soit premier.

Le nombre $M + 1 = 2^n$ ne contient que les facteurs 2^h, $(h \leqslant n)$. Considérons alors la série provenant de l'équation $x^2 - 4x + 1 = 0$, donnant $\Delta = 12$

$$\left(\frac{\Delta}{M}\right) = \left(\frac{12}{M}\right) = \left(\frac{3}{M}\right) = -\left(\frac{M}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

On aura donc

$$u_{M+1} = 0, \qquad \text{ou} \qquad u_{2n} = 0.$$

Mais

$$u_{2n} = v_{2n-1}.v_{2n-2}.v_{2n-3}. \ldots . v_4.v_2.v_1.u_1.$$

Or

$$u_1 = 1, \qquad v_1 = 4, \qquad v_2 = v_1^2 - 2, \qquad v_4 = v_2^2 - 2, \qquad \ldots$$

Ainsi la série

$$v_1 = 4, \qquad v_2 = v_1^2 - 2, \qquad v_4 = v_2^2 - 2, \qquad \ldots, \qquad (1)$$

ou par un changement de numérotage la série

$$v_1 = 4, \; v_2 = v_1^2 - 2, \; v_3 = v_2^2 - 2, \; \ldots \; v_i = v_{i-1}^2 - 2, \; (2)$$

finit par un terme nul, l'ordre de ce terme est au plus 2^{n-1} dans (1) ou n dans (2) [1].

Application. — Considérons le nombre

$$M_{257} = 2^{257} - 1 =$$

231584 178474 632390 847141 970017 375815 706539 969331 281128 078915 168015 826259 279871.

Si M_{257} est premier, on aura

$$v_{2k} \equiv 0 \text{ (Mod. M)}, \qquad \text{avec} \qquad k \leqq 256.$$

Or, partant de

$$v_1 = 4, \qquad v_{i+1} = v_i^2 - 2,$$

on ne trouve pas de terme congru à 0 (Mod. N_{257}). Il en résulte que, sauf erreur dans les calculs que nous avons effectués (août-décembre 1922), ce nombre est composé. Toutefois, on ne connaît pas les facteurs de ce nombre.

D'autre part, on n'a pas encore une confirmation de la non primalité de ce nombre.

14. Soit enfin, un nombre $N = k.2^n \pm 1$, k étant impair et relativement petit.

On considérera la série provenant de l'équation

$$x^2 - px + q = 0,$$

telle que

$$\left(\frac{\Delta}{k.2^n - 1}\right) = -1, \qquad \text{ou} \qquad \left(\frac{\Delta}{k.2^n + 1}\right) = +1,$$

alors, on aura

$$u_{k.2^n} \equiv 0.$$

Or

$$u_{k.2^n} = v_{k.2^{n-1}}.v_{k.2^{n-2}}. \ldots, v_{4k}.v_{2k}.v_k.u_k.$$

---

[1] Nous croyons devoir rappeler ici que Lucas a posé la question suivante : Démontrer *sans se servir de la table des nombres premiers* que $N = 2^{31} - 1$ est premier.

Il est hors de doute, qu'en posant cette question, Lucas avait en vue son procédé, que nous venons d'exposer. Mais on aurait eu une bonne solution aussi en prouvant que $a^{N-1} \equiv 1$ (Mod. N), avec $a = 3$. On aurait pu aussi prouver que l'équation indéterminée $x^2 - 2y^2 = N$, n'a qu'une seule solution avec $\sqrt{N} < x < \sqrt{2N}$ (T, II, XV). On peut encore *isoler* les résidus de N.

Mais c'est, nous semble-t-il, dénaturer la pensée de Lucas, que d'accepter la solution de Moret-Blanc (*Nouvelles Annales des Mathématiques*, 1881, p. 260), qui au lieu de se *servir* d'une table des nombres premiers, la *construit*.

D'une façon générale, u_k ainsi que v_k, sont différents de zéro. On passera de v_k à v_{2k}, de v_{2k} à v_{4k} et ainsi de suite par la formule de duplication

$$v_{2l} = v_l^2 - 2q^l \ .$$

Pour faciliter le calcul, on prendra $q = \pm 1$.

On trouvera un v nul. L'ordre de ce terme est au plus $k.2^{n-1}$. Il peut toutefois arriver qu'on ait $v_{2^{n-1}} \equiv 0$.

En général, il peut arriver que la relation $v_x \equiv 0$, ait lieu avec un indice x qui est un sous-multiple de $k.2^{n-1}$. On retombe alors, dans les inconvénients de la réciproque du théorème de Fermat.

Disons enfin, que dans le cas d'un nombre $N = k.2^n + 1$, nous préférons la réciproque du théorème de Fermat, parce qu'on passe plus facilement de a^x à a^{kx} que de v_x à v_{kx}.

CHAPITRE XII.

De l'équation $x^2 - y^2 = N$.

I. Formes linéaires de x.

1. L'équation $x^2 - y^2 = N$, est de la plus grande importance dans les questions de factorisation. A cause de sa forme particulière, il est facile de trouver les formes de x pour un module quelconque. Nous supposons dans ce qui suit qu'on prend pour module, un nombre premier impair.

Tout nombre premier peut être pris pour module, excepté 2, puisque pour le module 2, tout nombre est résidu. Au lieu du module 2, on prendra le module 2^n.

Pour ce qui est des autres nombres premiers, ils peuvent tous être utilisés directement. Toutefois, dans certains cas, on aura intérêt à recourir au module p^2, ou en général à p^n.

2. Théorème.— *Si* $\left(\frac{N}{p}\right) = -1$, *il y a* $\frac{p-1}{2}$ *valeurs* (*Mod.* p) *de* x *pouvant satisfaire à l'équation* $x^2 - y^2 = N$. *Pour toutes ces valeurs de* x, y *est différent de* 0.

Si $\left(\frac{N}{p}\right) = +1$, *il y a* $\frac{p+1}{2}$ *valeurs de* x (*Mod.* p) *pouvant satisfaire à l'équation* $x^2 - y^2 = N$. *Pour deux de ces valeurs* $y \equiv 0$, *mais* y *est différent de* 0 (*Mod.* p) *pour les* $\frac{p-3}{2}$ *autres valeurs de* x.

Dans cet énoncé p est supposé être un nombre premier impair.

En effet, si on pose $x + y \equiv i$, on doit prendre $x - y \equiv \frac{N}{i} \equiv j$ (Mod. p), i et j étant supposés compris entre 1 et $p - 1$

$$1 \leqslant i \quad \text{ou} \quad j \leqslant p - 1.$$

De ces deux congruences, on tirera la valeur (unique) de x (Mod. p).

On aura évidemment la même valeur de x en posant

$$x + y \equiv j, \qquad x - y \equiv \frac{N}{j} \equiv i \text{ (Mod. } p).$$

Il en résulte qu'aux $p-1$ valeurs possibles de $x+y$ correspondent $p-1$ valeurs possibles de $x-y$, mais ces $p-1$ couples de valeurs de $x+y$ et $x-y$ donnent lieu à $\frac{p-1}{2}$ valeurs différentes de x, tant que i et j seront différents. Il en sera ainsi en particulier, lorsque $\left(\frac{N}{p}\right)=-1$, puisque dans cas, on ne peut pas avoir $i=j$, car $i=j$ entraîne $y\equiv 0$ (Mod. p), ce qui donne $x^2\equiv N$ (Mod. p) ou $\left(\frac{N}{p}\right)=+1$.

Si, en deuxième lieu, on a $\left(\frac{N}{p}\right)=+1$, il existe encore $(p-1)$ valeurs possibles de $x+y$, auxquelles correspondent $(p-1)$ valeurs possibles de $(x-y)$. Mais deux des valeurs de $x+y$, se comportent autrement que les $p-3$ autres valeurs. Ce sont les deux valeurs de $x+y$ qui donnent $x-y\equiv x+y\equiv\sqrt{N}$ (Mod. p). Pour ces deux valeurs de $x+y$, on aura $y\equiv 0$ (Mod. p). Les $p-3$ autres valeurs de $x+y$, donnent lieu comme dans le premier cas à $\frac{p-3}{2}$ valeurs de x.

Ainsi, dans ce cas, on aura $\frac{p-3}{2}+2=\frac{p+1}{2}$ valeurs de x (Mod. p) [1].

Corollaires. — 1° Si $p\equiv 3$ (Mod. 4) et $\left(\frac{N}{p}\right)=-1$, on peut prendre $x\equiv 0$ (Mod. p), mais si $\left(\frac{N}{p}\right)=+1$, $x\equiv 0$, est inadmissible.

---

(1) On peut utiliser ces résultats pour déterminer le nombre de restes suivis de restes ou de non restes et inversement.

Ainsi, on trouve que dans la suite 1, 2, 3, ..., $(p-1)$, il y a $\frac{p-5}{4}$ restes suivis de restes, $\frac{p-1}{4}$ restes suivis de non restes, $\frac{p-1}{4}$ non restes suivis de restes et enfin $\frac{p-1}{4}$ non restes suivis de non restes, si $p\equiv 1$ (Mod. 4). Mais, si $p\equiv 3$ (Mod. 4), il y aura $\frac{p-3}{4}$ restes suivis de restes, $\frac{p+1}{4}$ restes suivis de non restes, $\frac{p-3}{4}$ non restes suivis de restes ou de non restes.

En effet, si $\left(\frac{N}{p}\right) = -1$, on aura $\frac{p-1}{2}$ valeurs de x ; or, $\frac{p-1}{2}$ est impair et toutes les valeurs de x, excepté 0, sont doubles, car si $x \equiv a$ (Mod. p), est une solution, $x \equiv -a$, l'est aussi, puisque l'équation $x^2 - y^2 = N$, est vérifiée quand on y remplace x par $-x$. Pour avoir un nombre impair de solutions, il faut prendre la solution $x \equiv 0$.

D'ailleurs, $x \equiv 0$, donne

$$y^2 \equiv 0 - N, \qquad \text{et} \qquad \left(\frac{-N}{p}\right) = -\left(\frac{N}{p}\right) = +1,$$

ce qui prouve que $x \equiv 0$, donne une solution admissible, si

$$\left(\frac{N}{p}\right) = -1.$$

Mais, si $\left(\frac{N}{p}\right) = +1$, on trouve que $x \equiv 0$, est inadmissible.

2° On trouve de même, si le module $p \equiv 1$ (Mod. 4), $x \equiv 0$ est une solution admissible si $\left(\frac{N}{p}\right) = +1$, et inadmissible si $\left(\frac{N}{p}\right) = -1$.

3. Théorème. — Si y n'est pas nul, il n'y a aucun avantage à se servir du module p^2, c'est-à-dire, toute solution (Mod. p), est aussi solution (Mod. p^2). Mais, si $y \equiv 0$, les solutions (Mod. p), peuvent être réduites (Mod. p^2).

On sait, en effet, que si la congruence $x^2 \equiv a$ (Mod. p) est possible, la congruence $x^2 \equiv a$ (Mod. p^2) l'est aussi, si a n'est pas $\equiv 0$. Mais, si $a \equiv 0$, de tous les multiples de p : $0, p, 2p, 3p, \ldots, (p-1)p$, seul le premier est résidu (Mod. p^2).

Si donc $y \equiv 0$ (Mod. p), on aura $y^2 \equiv 0$ (Mod. p^2) et l'équation $x^2 - y^2 = N$, devient $x^2 \equiv N$ (Mod. p^2), qui donne deux valeurs de x (Mod. p^2) et non (Mod. p).

Nous dirons que les solutions de x donnant y non $\equiv 0$, sont irréductibles. Mais les solutions de x donnant $y \equiv 0$ (Mod. p), sont réductibles.

4. Les formes linéaires de x, solutions de l'équation

$$x^2 - y^2 = N,$$

peuvent aussi être trouvées comme suit :

Posons

$$\pm\, x \equiv 0,\ 1,\ 2,\ 3,\ \ldots,\ \frac{p-1}{2}\ (\text{Mod. } p).$$

On trouvera en portant ces valeurs dans l'équation

$$x^2 - y^2 = N, \qquad y^2 \equiv x^2 - N \equiv c_0,\ c_1,\ c_2,\ c_3,\ \ldots.\ (\text{Mod, } p).$$

Certaines valeurs c_i seront résidus (Mod. p), les valeurs correspondantes de x sont des solutions éventuelles.

Mais si une valeur de x, $x = i$ conduit à $y = c_i$ et si $\left(\frac{c_i}{p}\right) = -1$, cette valeur de x est inadmissible.

Il en résulte certaines formes linéaires qui seront solutions de x dans $x^2 - y^2 = N$ et certaines autres qui ne le seront pas.

Si ensuite $\left(\frac{N}{p}\right) = +1$ et pour une certaine valeur de x, $x = i$, on a $y = 0$, considérons les valeurs

$$\pm x = i,\ p - i,\ p + i,\ 2p - i,\ 2p + i,\ \ldots,\ \frac{p-1}{2}\, p + i\ (\text{Mod. } p^2),$$

$$y^2 \equiv 0\ (\text{Mod. } p), \qquad \text{ou} \qquad y^2 \equiv kp\ (\text{Mod. } p^2),$$

$$k \equiv 0,\ 1,\ 2,\ 3,\ \ldots,\ p - 1\ (\text{à l'ordre près}).$$

De toutes ces valeurs de y^2 seule la valeur $y^2 \equiv 0$ (Mod. p^2) est résidu. Il en résulte que parmi les p valeurs considérées de x, seules deux sont des solutions.

Exemples numériques. 1° Soit

$$p = 11, \qquad \text{et} \qquad N \equiv 2\ (\text{Mod. } 11),$$

Si on pose

$$x + y \equiv 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ \ 9,\ 10$$

$$x - y \equiv 2,\ 1,\ 8,\ 6,\ 7,\ 4,\ 5,\ 3,\ 10,\ \ 9$$

$$\overline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}$$

$$x \equiv 7,\ \ 0,\ 5,\ 6,\qquad\qquad 4$$

Ainsi, les cinq solutions éventuelles de x sont

$$\pm\, x \equiv 0,\ 4,\ 5\ (\text{Mod. } 11).$$

Si on pose

$$\pm x \equiv 0,\ 1,\ 2,\ 3,\ 4,\ 5 \text{ (Mod. 11)}.$$

On trouve

$$y^2 \equiv x^2 - \mathrm{N} \equiv 9,\ 10,\ 2,\ 7,\ 3,\ 1$$

$$n,\ n,\ n.$$

Les valeurs $\pm x \equiv 1,\ 2$ ou 3,

conduisant à un non résidu (Mod. 11), sont inadmissibles, mais les valeurs

$$\pm x \equiv 0,\ 4,\ 5 \text{ (Mod. 11)},$$

conduisent à un résidu et sont parfaitement admissibles.

On trouve

$$y^2 \text{ non} \equiv 0, \qquad \text{ou} \qquad y \text{ non} \equiv 0 \text{ (Mod. } p).$$

2° Soit

$$p = 11, \qquad \mathrm{N} \equiv 3 \text{ (Mod. 11)}.$$

On prendra

$$x + y \equiv 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10$$

$$x - y \equiv 3,\ 7,\ 1,\ 9,\ 5,\ 6,\ 2,\ 10,\ 4,\ 8$$

d'où

$$x \equiv 2,\ 10,\ 1,\ 5,\ 6,\ 9$$

$$y \equiv 0,\ 0$$

On trouve

$$\frac{p-3}{2} = 4 \text{ valeurs de } x \text{ donnant } y \text{ non} \equiv 0,$$

et $\quad 2 \quad$ » $\quad x \quad$ » $\quad y \equiv 0.$

Soit en tout $\quad \dfrac{p+1}{2} = 6$ valeurs de x.

On trouvera ces mêmes six valeurs de x, en posant

$$\pm x \equiv 0,\ 1,\ 2,\ 3,\ 4,\ 5 \text{ (Mod. } p),$$

$$y^2 \equiv x^2 - \mathrm{N} \equiv 8,\ 9,\ 1,\ 6,\ 2,\ 0$$

$$n,\ n,\ n$$

Les valeurs $\pm x \equiv 0,\ 3,\ 4$ conduisant à un non résidu sont inadmissibles, les valeurs $\pm x \equiv 1,\ 2,\ 5$ conduisent à un résidu et sont admissibles.

Pour $\pm x \equiv 1,\ 2$ (Mod. 11), y non $\equiv 0$, mais pour $x \equiv \pm 5$, on trouve $y \equiv 0$. Les valeurs correspondantes de x peuvent être réduites.

Soit, pour fixer les idées, $\mathrm{N} \equiv 47$ (Mod. 121). Considérons les valeurs possibles $x = \pm 5$ (Mod. 11) pour le module $11^2 = 121$.

Posons donc

$$\pm x \equiv 5, \quad 6, 16, 17, 27, 28, 38, 39, 49, 50, 60 \text{ (Mod. 121)},$$

$$y^2 = x^2 - N \equiv 99, 110, 88, \quad 0, 77, 11, 66, 22, 55, 33, 44$$

Seul

$$x = \pm 17 \text{ (Mod. 121)} \qquad \text{conduit à} \qquad y^2 \equiv 0 \text{ (Mod. 121)}.$$

Par conséquent, on aura dans le cas de

$$N \equiv 47 \text{ (Mod. 121)}, \qquad \pm x \equiv 1, 2, 5 \text{ (Mod. 11)},$$

tant qu'on ne s'adresse pas au module 121. Mais, si on fait intervenir le module 121, on aura

$$\pm x \equiv 1, 2 \text{ (Mod. 11)}, \qquad \text{ou} \qquad x \equiv \pm 17 \text{ (Mod. 121)}.$$

5. Si le module est p et que $\left(\frac{N}{p}\right) = +1$, on aura une deuxième source d'élimination si on parvient à établir si $\left(\frac{\pm p}{N}\right) = +1$, ou -1.

Supposons d'abord que le module p soit de la forme $4k + 3$ et $\left(\frac{-p}{N}\right) = +1$.

Sans cette dernière condition, tous les cas

$$x + y \equiv 1, 2, 3, 4, \ldots, (p-1) \text{ (Mod. } p),$$

peuvent se présenter. A ces $p - 1$ valeurs possibles de $x + y$ correspondent $p - 1$ valeurs de $x - y$, d'où il résulte $\frac{p-3}{2}$ valeurs de x donnant y non $\equiv 0$ et deux valeurs de x donnant $y \equiv 0$.

Mais à cause de $\left(\frac{-p}{N}\right) = +1$, $x \pm y$ ne peut plus prendre que $\frac{p-1}{2}$ valeurs différentes (Mod. p) auxquelles correspondent $\frac{p-1}{2}$ valeurs différentes de $x \mp y$ qui donnent $\frac{p+1}{4}$ couples différents.

Par exemple, si $p = 11$ et $N \equiv 3$ (Mod. 11), on aura

$$\pm x \equiv 1, 2, 5.$$

Mais, si on a $\left(\frac{-11}{N}\right) = +1$, on ne peut avoir que

$$x + y \equiv 1,\ 3,\ 4,\ 5,\ 9 \text{ (Mod. 11)},$$

$$x - y \equiv 3,\ 1,\ 9,\ 5,\ 4$$

d'où $$x \equiv 1,\ 2,\ 5 \text{ (Mod. 11) (sans double signe)},$$

dont la dernière peut encore être réduite. Par exemple, si

$$N \equiv 47 \text{ (Mod. 121)}, \qquad \text{et} \qquad \left(\frac{-11}{N}\right) = +1,$$

on aura

$$x \equiv 1,\ 2 \text{ (Mod. 11)}, \qquad \text{ou} \qquad 104 \text{ (Mod. 121)}.$$

Ainsi, si le module p est de la forme $4k + 3$ et $\left(\frac{-p}{N}\right) = +1$, on peut limiter la valeur de x à $\frac{p+1}{4}$ cas (Mod. p).

On peut aussi dire que dans l'équation $x^2 - y^2 = N$, x aura $\frac{p+1}{4}$ solutions (Mod. p) si $\left(\frac{-p}{N}\right) = +1$.

De ces $\frac{p+1}{4}$ solutions une seule donne $y \equiv 0$ et cette solution peut être réduite (Mod. p^2). Les $\frac{p-3}{4}$ autres valeurs de y donnent y non $\equiv 0$ et sont irréductibles.

Une autre façon de représenter ces résultats, est la suivante :

Si le module est p de la forme $4k + 3$ et $\left(\frac{-p}{N}\right) = +1$, alors on aura $\frac{p-3}{2}$ solutions de x irréductibles et deux solutions réductibles, soit en tout $\frac{p+1}{2}$ solutions (Mod. p).

Ce nombre de solutions est pair et peut être mis sous la forme

$$\pm\, x \equiv a_1,\ a_2,\ a_3,\ \ldots,\ a_i \text{ (Mod. } p), \qquad i = \frac{p+1}{4}.$$

Ces $\frac{p+1}{4}$ valeurs peuvent être prises *avec le double signe*, tant qu'on ne fait pas usage de la relation $\left(\frac{-p}{N}\right) = +1$, mais

ces $\frac{p+1}{4}$ valeurs doivent être affectées *d'un signe précis*, si on tient compte de la relation $\left(\frac{-p}{N}\right) = +1$.

Par exemple, soit $p = 19$, $N \equiv 6$,

on aura $\pm x \equiv 2, 5, 6, 7, 8,$

ou $\pm x \equiv 5, 7, 8, 13, 17$ (Mod. 19) (10 solutions).

Mais, si dans les mêmes conditions, on parvient à établir que $\left(\frac{-19}{N}\right) = -1$, on aura

$$x \equiv 5, 7, 8, 13, 17 \text{ (Mod. 19) (5 solutions).}$$

6. Supposons maintenant que le module p soit de la forme $4k+1$ et $\left(\frac{N}{p}\right) = +1$. On aura alors $\frac{p+1}{2}$ valeurs de x, tant qu'on ne sait rien sur le symbole $\left(\frac{p}{N}\right)$.

Mais, si on sait que $\left(\frac{p}{N}\right) = +1$, le nombre de solutions de x, peut être réduit à $\frac{p+3}{4}$ ou $\frac{p-1}{4}$ suivant que $\left(\frac{N}{p}\right)_4 = +1$, ou -1, c'est-à-dire, suivant que N est ou n'est pas résidu biquadratique de p.

Soit, par exemple

$$p = 13, \qquad N \equiv 3 \text{ (Mod, 13).}$$

On peut poser

$$x + y \equiv 1, 2, 3, 4, \ 5, 6, 7, 8, 9, 10, 11, 12 \text{ (Mod. 13),}$$

$$x - y \equiv 3, 8, 1, 4, 11, 7, 6, 2, 9, 12, \ 5, 10$$

d'où $x \equiv 2, 5, \ 4, \ 8, 0, \ 9, 11.$

Mais, si $\left(\frac{p}{N}\right) = \left(\frac{13}{N}\right) = +1$, les facteurs de N doivent avoir la forme $26k \pm 1, 3, 9$ et on doit conserver les hypothèses suivantes

$$x + y \equiv 1, 3, 4, 9, 10, 12 \text{ (Mod. 13),}$$

$$x - y \equiv 3, 1, 4, 9, 12, 10$$

donnant $x \equiv 2, \ 4, 9, 11.$

On aura ainsi quatre solutions de x (Mod. 13) au lieu de sept.

Remarquons que 3 est un résidu biquadratique de 13

$$\left(\frac{3}{13}\right)_4 = +1.$$

Comme deuxième exemple, nous allons envisager le cas de $\left(\frac{p}{N}\right)_4 = -1$, par exemple celui de $p = 13$, $N \equiv 4$ (Mod. 13).

On trouve $\pm x = 0, 1, 2, 4$ (Mod. 13), soit sept solutions.

Mais, si dans ces mêmes conditions, on établit que $\left(\frac{13}{N}\right) = +1$, on aura

$$\pm x \equiv 0,\ 4 \text{ (Mod. 13), soit trois solutions.}$$

On remarquera que dans ce cas $\left(\frac{N}{p}\right)_4 = -1$, c'est-à-dire, N est un résidu quadratique de p, mais n'est pas un résidu biquadratique.

En effet, supposons qu'on ait $\left(\frac{p}{N}\right) = \left(\frac{N}{p}\right) = +1$, alors $x + y$, ainsi que $x - y$ peut avoir $\frac{p-1}{2}$ valeurs différentes, c'est-à-dire, on aura

$$x + y \equiv a_1, a_2, a_3, \ldots, a_i \text{ (Mod. } p), \qquad i = \frac{p-1}{2},$$

$$x - y \equiv b_1, b_2, \ldots, \qquad b_i$$

Considérons maintenant les deux cas qui peuvent se présenter.

1° $\left(\frac{N}{p}\right)_4 = +1$. Puisque $a_k b_k \equiv N$, on peut avoir $b_k \equiv a_k$.

Dans ce cas, les $\frac{p-1}{2}$ couples, donneront

$$2 + \frac{\frac{p-1}{2} - 2}{2} = \frac{p+3}{4} \text{ solutions de } x.$$

2° $\left(\frac{N}{p}\right)_4 = -1$. Dans ce cas, on ne peut pas avoir $b_k \equiv a_k$ et les $\frac{p-1}{2}$ couples conduisent à $\frac{p-1}{4}$ solutions de x.

Il est à remarquer que N étant résidu (Mod. p), on peut bien trouver $b_k = a_k$ et tel que $a_k b_k \equiv \mathrm{N}$, mais ces valeurs b_k et a_k seront telles que $\left(\frac{a_k}{p}\right) = \left(\frac{b_k}{p}\right) = -1$ et par conséquent inadmissibles pour $x + y$ ou $x - y$.

Ces résultats peuvent être énoncés autrement.

Si $\left(\frac{p}{\mathrm{N}}\right) = \left(\frac{\mathrm{N}}{p}\right) = +1$ et si $\left(\frac{\mathrm{N}}{p}\right)_4 = +1$, le nombre des solutions de x est $\frac{p+3}{4}$, mais deux de ces solutions peuvent être réduites (Mod. p^2), les $\frac{p+3}{4} - 2 = \frac{p-5}{4}$ autres sont irréductibles.

Si, dans les mêmes conditions $\left(\frac{\mathrm{N}}{p}\right) = -1$, le nombre de solutions de x est $\frac{p-1}{4}$ et ces solutions sont toutes irréductibles.

Sous cette forme, l'énoncé se rapproche de celui du n° 2 de ce chapitre.

7. Nous allons appliquer les considérations générales qui précèdent à quelques cas simples, en examinant successivement les modules impairs inférieurs à 70.

Commençons par le module le plus petit et aussi le plus important, c'est-à-dire, par le cas de $p = 3$.

Soit d'abord $\mathrm{N} \equiv 2$, alors x aura $\frac{p-1}{2} = 1$, seule solution celle de $x \equiv 0$. Cette solution est irréductible.

Si ensuite $\mathrm{N} \equiv 1$ (Mod. 3), on aura $\frac{p+1}{2} = 2$ solutions de x, soit $x \equiv \pm 1$. Ces deux solutions sont réductibles, quand on fait intervenir le module 9.

Considérons à cet effet, les cas possibles (Mod. 9).

Si	$\mathrm{N} \equiv 1$,	on aura	$x \equiv \pm 1$,
	4,		2,
	7,		4.

On aura ainsi deux solutions (Mod. 9), au lieu de deux solutions (Mod. 3).

Ces deux solutions module 9, peuvent être réduites module 27, ou module 81, ou module 243, etc.

On trouvera une table de ces résultats dans notre Tome I, p. 190.

Nous allons examiner ce que deviennent ces solutions, quand on connaît le résidu — 3 de N, c'est-à-dire $\left(\frac{-3}{N}\right) = +1$.

Cela ne peut arriver que si $N \equiv 1$ (Mod. 3).

Alors, on aura $x \equiv +1$ (mais non ± 1). On aura donc une solution réductible (Mod. 9).

Si $N \equiv 1$ et $\left(\frac{-3}{N}\right) = +1$, on aura $x \equiv +1$ (Mod. 9),

4 7,

7 4.

On aura ainsi une solution (Mod. 9) et cette solution peut encore être réduite (Mod. 27, ou 81, etc.).

Examinons maintenant le module 5.

Si $N \equiv 2$ ou 3, on aura $\frac{p-1}{2} = 2$ valeurs de x ($x \equiv \pm 1$ ou ± 2). Mais, si $N \equiv 1$ ou 4, on aura $\frac{p+1}{2} = 3$ valeurs de x.

Si $N \equiv 1$, $x \equiv \pm 0, 1$,

4, 0, 2.

La solution $x \equiv 0$ est irréductible, mais les autres sont réductibles (Mod. 25) et on aura :

Si $N \equiv 1$ (Mod, 5), $x \equiv 0$ (Mod. 5), ou $\sqrt{N}$ (Mod. 25) (T, I, p. 191),

4 0 (Mod. 5), $\sqrt{N}$ (Mod. 25).

On aura ainsi une solution (Mod. 5), plus deux solutions (Mod. 25).

Si, de plus, on parvient à établir que $\left(\frac{5}{N}\right) = +1$, on aura les résultats suivants :

$$N \equiv 1, \quad \left(\frac{5}{N}\right) = 1, \quad x \equiv \sqrt{N} \text{ (Mod. 25)},$$
$$4, \quad x \equiv 0 \text{ (Mod. 5)}.$$

On trouvera de même dans le cas du module 7.

Si $N \equiv 3, \quad x \equiv 0, 2,$
$5, \quad 0, 3,$
$6, \quad 0, 1.$

On aura dans ce cas $\frac{p-1}{2} = 3$ solutions irréductibles.

Si $N \equiv 1, \quad x \equiv \pm 1, 3,$
$2, \quad 2, 3,$
$4, \quad 1, 2.$

Dans ce cas, on aura $\frac{p+1}{2} = 4$ solutions dont 2 irréductibles.

On peut aussi les écrire sous la forme suivante

$N \equiv 1, \quad x \equiv \pm 3$ (Mod. 7), ou $\sqrt{N}$ (Mod. 49),
$2, \quad 2 \quad \sqrt{N}$
$4, \quad 1 \quad \sqrt{N}$ (T, I, p. 192).

Si, de plus, on a établi que $\left(\frac{-7}{N}\right) = +1$, on aura

$N \equiv 1, \quad x \equiv +1, 3$ (Nod. 7),
$2, \quad 4, 5$
$4, \quad 2, 6$

soit $\frac{p+1}{2} = 2$ solutions (Mod. 7), qu'on peut remplacer par une solution (Mod. 7) et une solution (Mod. 49).

On trouverait des résultats analogues, pour les autres modules. Nous nous bornerons à donner la table des solutions de x dans les différents cas de modules impairs et < 70.

TABLE DE SOLUTIONS DE x DANS L'ÉQUATION $x^2 - y^2 = N$.

Premier cas. $\left(\frac{N}{p}\right) = -1$.

Toutes les valeurs de x sont irréductibles.

p	N	$\pm x$
3	2	0
5	2	1
	3	2
7	3	0 2
	5	0 3
	6	0 1
11	2	0 4 5
	6	0 2 3
	7	0 1 4
	8	0 1 3
	10	0 2 5
13	2	1 4 5
	5	1 2 3
	6	3 4 6
	7	2 4 6
	8	2 3 5
	11	1 5 6
17	3	1 2 4 6
	5	1 2 3 8
	6	2 5 6 7
	7	3 4 5 7
	10	1 3 5 6
	11	3 6 7 8
	12	2 4 5 8
	14	1 4 7 8
19	2	0 3 5 7 8
	3	0 1 2 3 8
	8	0 3 5 6 9
	10	0 4 6 7 8
	12	0 2 3 4 6
	13	0 1 6 7 9
	14	0 1 2 5 7
	15	0 1 4 8 9
	18	0 2 4 5 9
23	5	0 3 6 8 10 11
	7	0 3 4 5 6 10
	10	0 4 6 7 8 9
	11	0 1 2 6 9 11
	14	0 2 3 4 7 8
	15	0 1 2 4 8 10
	17	0 5 7 8 9 11
	19	0 2 3 5 9 10
	20	0 1 3 6 7 11
	21	0 1 2 4 5 11
	22	0 1 5 7 9 10
29	2	1 3 5 6 8 13 14
	3	2 3 4 5 6 9 12
	8	1 2 3 6 10 12 13
	10	1 2 3 4 8 9 11
	11	2 4 6 7 8 11 13
	12	4 5 6 8 10 11 12
	14	1 3 6 7 9 10 11
	15	3 4 7 8 12 13 14
	17	1 2 4 9 10 13 14
	18	3 5 9 10 11 13 14
	19	5 7 8 9 10 12 13
	21	1 4 5 7 11 12 14
	26	1 2 5 7 8 10 14
	27	2 6 7 9 11 12 14

p	N	± x							
31	3	0	2	6	9	10	11	14	15
	6	0	4	5	10	12	13	14	15
	11	0	4	5	6	7	9	12	15
	12	0	1	3	4	9	11	12	13
	13	0	1	7	8	10	12	13	14
	15	0	2	3	4	5	8	9	12
	17	0	2	5	6	7	8	9	13
	21	0	2	3	5	7	11	14	15
	22	0	1	3	4	6	9	10	14
	23	0	1	5	8	11	12	14	15
	24	0	1	3	5	7	8	10	11
	26	0	2	3	6	8	11	12	13
	27	0	1	2	4	6	11	13	14
	29	0	4	6	7	8	10	13	15
	30	0	1	2	3	7	9	10	15
37	2	1	3	6	7	8	14	15	17	18
	5	1	2	3	4	7	10	12	13	17
	6	3	4	6	8	9	11	12	15	16
	8	1	2	3	6	7	9	12	14	16
	13	1	2	3	4	5	7	11	15	16
	14	2	5	9	10	11	13	14	15	17
	15	2	4	5	6	7	8	10	14	15
	17	1	4	8	9	10	11	12	13	18
	18	3	5	8	9	13	14	16	17	18
	19	3	4	7	9	10	11	15	17	18
	20	2	3	4	6	8	11	13	14	17
	22	1	5	7	10	11	12	13	14	16
	23	4	7	8	9	10	12	14	16	17
	24	5	6	7	8	12	13	15	16	18
	29	1	2	5	6	10	12	15	17	18
	31	1	2	8	11	13	15	16	17	18
	32	2	4	5	6	9	12	13	14	18
	35	1	3	5	6	9	10	11	16	18

p	N	± x								
41	3	1	2	6	7	8	9	11	12	13	17
	6	1	2	4	7	11	13	16	13	18	20
	7	3	4	5	7	8	9	11	13	14	17
	11	1	3	4	6	12	14	15	16	17	20
	12	2	4	7	12	14	15	16	17	18	19
	13	2	3	6	7	8	10	12	13	19	20
	14	2	3	4	8	10	11	13	14	16	18
	15	4	5	6	8	9	13	15	16	19	20
	17	1	3	4	5	7	9	10	12	18	19
	19	1	3	8	9	10	11	12	15	16	18
	22	1	2	8	9	10	12	14	15	17	20
	24	1	2	4	5	7	8	9	14	15	19
	26	1	4	5	6	7	10	12	13	16	20
	27	2	3	5	6	8	10	14	17	18	20
	28	6	7	8	10	13	14	15	16	18	19
	29	2	3	5	7	11	12	15	18	19	20
	30	3	5	9	11	12	13	14	15	16	20
	34	1	3	4	5	6	10	11	14	17	19
	35	2	5	6	9	11	16	17	18	19	20
	38	1	6	9	10	11	13	15	17	18	19
43	2	0	4	5	7	9	12	13	18	19	20	21
	3	0	1	2	3	4	9	10	14	16	19	20
	5	0	3	4	6	7	8	10	12	13	16	21
	7	0	2	4	8	9	14	17	18	19	20	21
	8	0	1	3	5	7	8	10	14	17	18	19
	12	0	2	3	4	5	6	8	11	15	18	20
	18	0	4	7	11	12	14	15	16	17	20	21
	19	0	1	4	5	6	10	11	13	18	19	21
	20	0	1	6	8	11	12	14	16	17	19	20
	22	0	2	6	9	10	11	12	15	17	18	19
	26	0	2	6	7	8	10	11	13	14	16	18
	27	0	1	3	5	6	9	12	13	14	16	17
	28	0	1	3	4	5	7	8	9	15	16	18
	29	0	1	3	8	9	11	13	14	15	19	21
	30	0	1	2	5	6	13	15	16	17	18	21
	32	0	2	5	6	7	9	10	14	15	16	20
	33	0	1	2	5	7	8	10	12	17	20	21
	34	0	1	2	4	7	9	10	11	12	13	17
	37	0	2	3	5	9	11	12	15	16	19	21
	39	0	3	6	7	8	13	15	17	19	20	21
	42	0	3	4	10	11	12	13	14	15	18	20

p	N	$\pm x$											
47	5	0	3	8	10	14	15	16	17	18	19	22	23
	10	0	4	8	9	11	13	15	18	20	21	22	23
	11	0	1	5	6	8	10	11	13	19	21	22	23
	13	0	4	5	7	8	9	11	12	14	15	16	22
	15	0	2	4	6	7	8	11	16	18	19	20	21
	19	0	2	3	5	6	10	11	13	14	15	16	22
	20	0	1	3	6	9	11	13	15	16	17	19	20
	22	0	3	5	6	7	8	9	12	13	17	20	23
	23	0	1	2	5	11	12	14	15	19	20	21	23
	26	0	2	4	9	10	11	12	13	16	17	18	19
	29	0	3	4	6	10	12	15	17	19	20	21	22
	30	0	1	2	5	6	8	9	14	15	17	18	19
	31	0	1	3	4	7	9	14	15	16	19	21	23
	33	0	2	6	7	9	12	13	15	17	18	21	22
	35	0	2	3	4	5	6	7	10	15	18	20	23
	38	0	3	4	5	11	12	13	14	17	18	21	23
	39	0	1	2	3	4	8	9	10	13	14	18	20
	40	0	1	3	5	7	8	11	16	17	18	21	22
	41	0	1	6	7	10	12	13	14	16	18	21	23
	43	0	2	7	8	12	13	14	16	19	20	22	23
	44	0	1	2	3	5	9	10	12	16	20	21	22
	45	0	1	2	4	5	7	9	10	17	19	22	23
	46	0	1	4	6	7	8	10	11	12	14	17	20
53	2	1	3	7	8	11	12	15	16	18	21	24	25	26
	3	2	3	4	7	9	10	13	15	19	22	23	24	26
	5	1	2	3	4	7	8	10	11	18	19	20	23	25
	8	1	2	3	5	6	11	14	16	17	21	22	23	24
	12	1	4	5	6	7	8	9	14	15	18	20	23	26
	14	1	2	5	11	12	13	15	17	19	20	22	23	25
	18	1	3	5	8	9	10	17	19	20	21	22	24	25
	19	2	3	5	6	9	10	11	13	15	16	18	19	20
	20	2	3	4	6	7	8	13	14	15	16	17	20	22
	21	2	5	6	7	8	9	11	12	13	14	18	21	24
	22	3	4	8	9	10	11	12	14	15	18	20	22	24
	23	4	6	10	12	13	15	17	18	20	21	22	23	26
	26	1	3	4	5	6	8	11	13	14	15	19	21	25
	27	4	6	8	9	12	13	14	16	19	21	23	25	26
	30	1	6	10	11	14	15	17	18	19	20	21	24	26
	31	4	5	10	11	12	14	16	17	18	22	24	25	26
	32	2	4	5	6	7	9	10	11	12	19	21	22	25
	33	2	3	4	7	14	16	17	19	20	21	24	25	26
	34	3	5	7	9	10	12	13	16	17	18	19	21	26
	35	5	6	8	9	13	16	17	18	20	22	23	24	25
	39	1	7	8	9	11	12	13	17	19	20	23	24	26
	41	1	2	4	5	9	10	14	15	17	21	23	25	26
	45	1	3	4	6	7	9	12	16	20	21	22	23	24
	48	1	2	7	8	10	12	13	14	16	17	18	23	25
	50	1	2	5	7	13	14	15	16	18	19	22	24	26
	51	2	3	6	8	10	11	12	15	16	22	23	25	26

p	N	$\pm x$														
59	2	0	3	8	9	11	13	14	15	17	18	19	21	26	27	28
	6	0	2	3	5	9	10	12	13	19	21	23	25	26	27	29
	8	0	3	5	6	7	16	17	18	21	22	23	25	26	28	29
	10	0	2	5	6	9	12	13	14	18	20	24	25	26	28	29
	11	0	1	3	4	6	8	11	12	16	20	21	22	23	26	29
	13	0	4	5	7	8	9	10	11	15	16	18	19	21	25	28
	14	0	1	2	6	7	10	11	12	14	18	22	25	27	28	29
	18	0	2	4	5	8	9	14	17	19	20	22	24	25	26	27
	23	0	3	7	8	12	13	14	21	22	24	25	26	27	28	29
	24	0	1	4	5	6	7	9	10	13	17	18	20	21	24	26
	30	0	4	7	9	13	14	16	19	20	21	22	23	24	25	28
	31	0	1	5	6	13	15	16	17	18	19	20	23	25	27	28
	32	0	1	3	6	7	9	10	12	13	14	15	17	23	25	27
	33	0	1	3	5	6	7	9	11	14	15	16	17	24	26	29
	34	0	1	2	4	7	10	11	12	13	16	17	20	21	25	27
	37	0	2	7	8	10	11	12	14	17	18	19	20	23	25	26
	38	0	1	2	5	6	8	10	16	17	19	21	23	24	26	29
	39	0	1	3	4	5	8	12	13	15	18	19	20	21	27	29
	40	0	1	3	4	7	9	10	11	12	18	19	23	24	26	28
	42	0	2	3	6	7	8	11	13	14	18	20	21	22	23	24
	43	0	1	2	3	5	8	10	11	14	15	16	18	20	22	25
	44	0	1	2	6	7	8	12	13	14	15	16	19	22	24	27
	47	0	2	3	4	6	8	10	11	13	15	18	19	24	28	29
	50	0	4	6	11	12	13	14	15	16	17	19	22	23	26	28
	52	0	3	8	9	10	14	16	17	18	20	21	22	23	27	29
	54	0	2	4	6	9	10	15	16	19	20	22	23	27	28	29
	55	0	1	4	5	7	8	9	10	11	17	22	24	27	28	29
	56	0	1	2	3	4	5	9	12	14	15	20	22	23	24	28
	58	0	2	4	5	11	12	14	15	16	21	24	25	26	27	29
61	2	1	4	6	7	8	11	12	13	21	23	24	25	26	27	29
	6	1	3	5	8	9	12	13	15	17	18	25	26	27	28	29
	7	2	4	7	8	9	12	16	18	19	20	23	24	28	29	30
	8	2	3	7	8	9	11	12	13	14	15	16	19	22	24	26
	10	1	3	5	7	12	14	18	19	21	22	25	26	27	28	30
	11	4	5	6	9	11	13	16	17	19	21	22	24	25	27	28
	17	1	2	4	6	8	9	10	12	14	15	16	19	21	26	27
	18	2	3	8	11	12	14	17	18	20	21	22	24	25	26	28
	21	1	3	4	5	6	9	11	12	16	20	22	23	26	29	30
	23	1	2	3	6	8	9	10	12	15	17	18	21	22	24	29
	24	2	3	5	6	7	9	10	11	16	18	24	25	26	27	30
	26	1	2	5	10	11	12	14	15	16	17	21	23	24	29	30
	28	1	3	4	5	8	13	14	15	16	18	21	23	24	25	29
	29	2	3	4	5	7	9	14	15	17	19	20	21	23	25	29
	30	4	5	7	8	10	15	17	20	21	22	24	25	26	28	30
	31	2	3	4	6	12	13	16	17	18	19	20	24	25	27	30
	32	4	6	9	13	14	16	17	18	22	23	24	26	28	29	30
	33	6	7	9	11	13	14	15	17	18	20	21	27	28	29	30
	35	1	4	6	7	9	10	11	12	13	14	18	20	22	25	29
	37	1	5	6	7	8	12	15	16	19	20	22	23	25	28	30
	38	2	4	5	10	11	12	13	14	15	18	20	22	23	27	28
	40	1	2	5	6	7	9	10	11	14	17	19	23	24	25	28
	43	1	2	3	4	10	13	15	19	20	22	24	27	28	29	30
	44	5	7	8	10	11	12	13	17	18	19	22	23	26	27	29
	50	1	2	3	4	5	6	7	8	13	17	20	21	23	26	30
	51	2	3	6	8	10	11	13	15	16	19	25	26	28	29	30
	53	1	2	7	10	16	18	19	20	21	22	23	26	27	28	29
	54	3	7	9	10	14	15	16	17	20	22	23	24	25	26	27
	55	3	4	6	8	10	11	14	15	18	19	21	23	27	28	30
	59	1	5	8	9	10	11	13	14	16	17	19	20	21	27	30

p	N	± x																
67	2	0	4	5	7	8	13	14	15	17	18	19	21	26	29	31	32	33
	3	0	1	2	3	5	6	14	15	19	20	21	24	25	27	30	32	33
	5	0	3	8	9	11	15	17	19	20	22	23	24	25	26	27	30	32
	7	0	2	4	6	10	11	14	15	17	18	19	24	25	28	30	31	33
	8	0	1	3	5	8	9	10	14	15	16	25	26	28	29	30	31	33
	11	0	2	3	5	6	10	13	17	19	20	22	23	24	26	28	29	33
	12	0	1	2	3	4	6	7	10	12	13	17	19	25	27	28	29	30
	13	0	1	6	7	9	12	13	14	21	23	25	26	29	30	31	32	33
	18	0	4	10	11	12	13	15	16	20	21	22	24	25	26	28	29	32
	20	0	3	6	7	13	15	16	17	18	19	21	22	23	27	29	30	33
	27	0	3	4	5	6	7	8	9	10	14	15	18	22	23	25	29	32
	28	0	1	4	5	7	8	11	12	17	19	20	22	28	29	30	31	33
	30	0	5	6	7	11	12	16	18	20	21	24	25	27	28	31	32	33
	31	0	1	2	8	11	13	15	16	18	19	23	24	28	29	30	31	32
	32	0	1	2	5	6	7	9	10	11	15	16	17	18	20	28	30	32
	34	0	2	4	7	9	13	16	17	18	19	23	24	25	26	27	30	31
	38	0	2	5	6	8	10	11	12	13	14	16	19	21	23	26	27	28
	41	0	3	6	8	9	10	12	14	16	17	18	20	21	23	28	30	31
	42	0	1	2	8	9	12	13	15	18	20	21	22	24	25	27	29	30
	43	0	1	3	4	5	6	7	8	13	14	20	22	23	24	27	28	31
	44	0	1	4	6	9	10	11	12	15	19	20	21	23	26	27	29	33
	45	0	1	2	5	7	8	9	10	11	14	16	22	23	24	27	29	33
	46	0	1	2	4	9	10	13	14	16	18	19	20	21	22	23	28	32
	48	0	2	4	6	7	8	9	11	12	13	14	17	20	24	26	29	33
	50	0	2	3	4	8	11	18	20	21	23	25	26	27	28	29	31	32
	51	0	1	3	7	10	12	15	16	17	20	21	23	24	26	31	32	33
	52	0	1	2	3	5	7	9	12	14	15	17	18	21	24	25	26	28
	53	0	1	3	5	10	11	12	13	14	17	19	22	24	25	27	31	32
	57	0	2	3	4	5	7	9	11	16	19	21	22	26	29	30	31	32
	58	0	1	4	8	9	12	14	15	16	18	19	22	24	26	27	28	33
	61	0	2	3	4	7	10	11	12	14	18	20	22	27	30	31	32	33
	63	0	5	6	8	10	12	13	16	17	18	22	23	25	26	30	32	33
	66	0	3	4	5	6	8	9	11	13	15	16	17	21	22	25	27	31

Deuxième cas. $\left(\frac{N}{p}\right) = +1$.

1° Modules de la forme $4k + 3$.

Les solutions doivent être prises avec le double signe, si on ne sait rien sur le symbole $\left(\frac{-p}{N}\right)$. Elles doivent être prises avec le signe $+$, si $\left(\frac{-p}{N}\right) = +1$.

Seule la solution $x \equiv \sqrt{N}$ est réductible.

p	N	x
3	1	1
7	1	1 3
	2	4 5
	4	2 6
11	1	1 7 9
	3	1 2 5
	4	4 8 9
	5	3 4 6
	9	3 5 10
19	1	1 9 11 13 14
	4	1 10 12 16 17
	5	3 4 5 9 12
	6	5 7 8 13 17
	7	2 4 7 10 11
	9	5 11 15 16 18
	11	1 3 6 7 15
	16	4 6 14 17 18
	17	2 6 8 9 16
23	1	1 2 3 5 7 17
	2	7 8 11 13 18 21
	3	2 9 11 16 19 20
	4	2 4 6 10 11 14
	6	1 12 13 14 15 20
	8	3 13 14 16 19 22
	9	3 5 6 9 15 21
	12	4 9 15 17 18 22
	13	6 7 10 12 18 19
	16	4 5 8 12 20 22
	18	1 8 10 16 17 21

p	N	x
31	1	1 3 6 8 9 15 17 19
	2	2 8 10 12 17 24 27 28
	4	2 3 6 7 12 16 18 30
	5	3 8 10 13 14 22 25 26
	7	4 10 15 18 26 28 29 30
	8	3 4 16 17 20 23 24 25
	9	4 5 7 11 13 17 22 28
	10	2 11 14 18 19 21 22 24
	14	1 7 15 18 20 22 23 27
	16	1 4 5 6 12 14 24 29
	18	1 7 9 11 12 21 25 26
	19	9 10 11 16 19 23 27 29
	20	6 13 16 19 20 21 26 28
	25	2 5 9 13 14 15 23 30
	28	5 8 20 21 25 27 29 30
43	1	1 4 6 19 21 27 28 29 31 33 38
	4	1 5 10 20 24 28 30 31 32 35 41
	6	1 12 15 19 25 26 27 35 36 39 41
	9	2 5 15 23 25 29 30 31 36 40 42
	10	4 5 11 14 15 17 18 22 27 33 35
	11	5 6 7 8 11 12 21 24 29 40 41
	13	6 7 9 10 14 19 22 23 25 28 42
	14	9 10 12 17 18 22 29 32 36 38 40
	15	6 8 14 15 17 20 30 31 34 38 39
	16	3 4 16 22 23 24 26 30 33 38 41
	17	3 8 9 10 13 15 18 24 26 27 31
	21	4 10 11 20 26 34 35 37 38 40 42
	23	1 2 4 8 9 12 14 21 25 30 37
	24	4 5 8 13 14 16 19 32 34 36 41
	25	7 13 17 23 24 26 27 32 34 37 38
	31	1 2 3 11 13 16 17 20 22 25 29
	35	1 7 11 16 18 19 23 31 37 39 40
	36	2 6 13 14 24 26 28 33 36 39 40
	38	3 9 11 17 21 28 36 37 39 41 42
	40	7 9 13 15 16 20 21 32 33 35 42
	41	2 3 6 10 12 16 18 21 23 34 35

p	N	x														
47	1	1	2	3	5	7	8	13	15	17	26	33	35			
	2	2	7	9	10	11	14	21	25	35	41	43	44			
	3	2	12	13	15	16	20	24	30	36	37	39	44			
	4	2	4	5	6	10	14	16	19	23	26	30	34			
	6	11	14	17	18	22	24	26	27	37	38	44	46			
	7	4	7	17	19	20	25	31	33	34	38	42	44			
	8	3	4	14	18	20	22	23	28	35	39	41	42			
	9	3	4	5	6	9	11	15	21	24	31	39	45			
	12	1	4	13	24	25	26	27	30	31	32	40	41			
	14	2	3	12	25	26	28	29	31	34	39	43	46			
	16	4	5	8	10	12	13	20	21	28	32	38	46			
	17	8	9	10	16	17	20	24	26	29	40	42	45			
	18	6	11	16	21	27	28	29	30	33	35	38	42			
	21	1	5	11	16	18	20	32	33	34	37	40	43			
	24	1	5	7	22	27	28	29	34	36	41	44	45			
	25	7	9	11	12	13	19	22	23	29	32	37	42			
	27	1	6	13	14	17	23	25	36	38	39	43	45			
	28	3	8	14	15	19	21	29	34	37	38	40	41			
	32	6	8	9	18	23	31	35	36	37	40	44	46			
	34	9	12	15	16	18	23	25	27	33	41	45	46			
	36	1	6	8	10	12	15	18	22	30	31	42	43			
	37	2	10	17	19	21	22	27	32	33	36	39	40			
	42	3	7	18	19	24	30	32	35	36	43	45	46			
59	1	1	2	7	9	12	31	32	33	38	39	41	43	51	53	55
	3	2	7	13	19	21	22	29	41	43	44	45	48	50	54	58
	4	3	8	12	16	32	35	36	40	41	42	45	52	54	56	57
	5	3	5	10	16	22	26	31	32	39	42	46	47	48	50	51
	7	4	12	14	15	18	19	21	25	33	37	42	50	51	53	58
	9	3	5	11	21	27	34	35	36	37	40	41	47	53	55	58
	12	1	2	10	15	17	18	21	22	28	30	32	33	36	45	55
	15	1	2	3	4	8	9	10	13	14	25	26	29	40	43	53
	16	4	6	10	14	27	28	34	35	36	38	43	45	48	51	54
	17	2	3	6	9	11	12	16	19	27	28	30	35	39	41	42
	19	9	10	16	20	24	25	28	38	44	45	47	51	53	56	58
	20	7	15	16	18	22	24	26	27	34	39	40	49	53	54	56
	21	5	6	7	10	11	12	15	20	23	27	29	38	40	45	50
	22	2	4	5	9	15	22	23	33	41	43	46	47	49	52	56
	25	1	5	13	18	28	29	35	37	38	39	40	42	45	47	49
	26	11	12	18	20	22	25	26	30	35	42	43	44	46	49	55
	27	4	5	6	7	11	14	17	21	26	28	32	39	44	56	57
	28	2	9	12	16	17	18	21	23	29	31	34	35	44	51	52
	29	6	13	14	15	20	24	26	29	32	36	41	49	51	52	55
	35	5	6	8	9	13	18	22	25	27	31	33	36	48	57	58
	36	2	5	8	12	17	24	36	37	38	44	46	48	49	50	53
	41	1	3	20	21	23	24	28	33	34	40	42	44	48	49	57
	45	7	8	9	15	19	20	23	26	30	32	34	35	37	48	58
	46	3	4	11	13	17	19	20	22	30	34	38	50	52	53	57
	48	3	8	15	17	23	25	28	29	39	46	52	54	55	57	58
	49	3	4	6	7	17	25	30	31	37	40	45	47	49	51	54
	51	1	10	19	21	24	26	27	31	37	43	45	46	52	56	57
	53	1	13	14	16	17	23	25	27	30	35	41	48	50	55	56
	57	1	7	8	11	14	16	19	20	29	31	33	36	46	47	54

p	N	x																
67	1	1	4	6	12	19	29	31	33	42	43	44	45	47	49	51	52	62
	4	1	5	9	10	29	30	32	36	40	43	44	46	48	50	55	59	65
	6	1	2	4	5	12	16	17	20	22	25	26	31	37	44	46	53	54
	9	2	5	8	10	15	31	35	41	45	47	48	49	54	55	60	64	66
	10	6	8	15	19	20	30	32	39	40	46	54	55	57	58	60	62	63
	14	3	9	11	21	22	29	30	36	39	41	43	52	54	57	60	61	66
	15	5	6	8	12	16	21	22	24	29	30	35	50	52	53	56	63	65
	16	3	4	7	9	16	24	34	38	42	46	47	48	49	54	57	62	65
	17	8	9	10	11	12	17	18	19	24	33	36	41	45	46	61	64	65
	19	6	9	10	11	13	16	26	31	34	35	37	40	43	49	62	63	66
	21	1	3	11	13	17	24	25	28	29	35	44	49	55	58	61	62	63
	22	2	3	6	9	16	19	21	25	27	28	32	33	36	38	45	53	55
	23	7	10	12	14	15	17	21	22	27	30	36	38	39	43	44	49	63
	24	5	15	17	23	26	27	28	33	35	42	43	46	57	59	60	63	65
	25	7	8	13	23	25	33	36	37	39	43	46	47	48	53	56	58	62
	26	9	13	15	19	22	24	26	27	31	32	39	47	50	51	53	60	61
	29	1	4	8	11	13	14	15	16	20	21	33	37	42	48	50	57	64
	33	1	10	17	18	21	22	28	38	40	41	42	48	51	53	56	66	62
	35	7	15	18	21	25	31	33	40	44	45	54	56	57	59	61	65	66
	36	2	5	6	14	24	26	36	37	38	40	44	47	51	52	57	63	64
	37	3	5	12	13	14	15	19	23	28	29	32	34	37	40	41	49	56
	39	6	7	11	17	20	21	23	24	29	32	48	49	51	53	59	64	66
	40	3	7	8	10	14	18	20	24	26	27	29	37	42	51	54	55	56
	47	2	3	4	6	13	14	18	22	30	33	35	39	41	43	46	59	66
	49	1	6	20	25	27	34	35	37	38	39	41	45	50	51	59	60	65
	54	1	2	7	16	19	23	31	39	41	42	52	55	56	59	61	63	64
	55	2	12	15	16	18	27	28	29	34	36	47	50	54	58	59	62	64
	56	2	9	12	14	20	23	25	26	30	45	48	49	52	56	60	61	12
	59	1	3	4	5	11	17	18	21	23	26	30	34	39	40	45	47	58
	60	4	7	8	9	19	22	23	25	28	30	34	35	43	51	53	57	64
	62	4	13	14	16	17	27	32	34	44	52	55	56	58	60	64	65	66
	64	4	9	10	19	20	26	35	36	38	40	42	49	50	53	59	61	66
	65	10	11	14	22	23	25	28	31	32	33	38	47	50	52	54	58	65

2° Modules de la forme $4k + 1$.

On prendra les valeurs de x et x', si on ne sait rien sur le symbole $\left(\frac{p}{N}\right)$.

Si on sait que $\left(\frac{p}{N}\right) = +1$, on prendra les valeurs de x'.

Seule la solution x ou $x' = \sqrt{N}$ est réductible.

p	N	$\pm x$	$\pm x'$
5	1	0	1
	4	2	0
13	1	0 2	1 6
	3	0 5	2 4
	4	1 2	0 4
	9	0 6	3 5
	10	3 6	0 1
	12	4 5	0 3
17	1	4 6	0 1 3
	2	0 1 6	2 7
	4	5 8	0 2 6
	8	0 2 5	3 4
	9	0 3 8	1 5
	13	2 3	0 7 8
	15	0 4 7	6 8
	16	1 7	0 4 5
29	1	0 5 6 8	1 9 11 13
	4	2 3 7 11	0 10 12 13
	5	2 5 11 12	0 1 3 8
	6	1 8 12 14	0 6 10 11
	7	0 1 7 10	4 6 8 9
	9	2 3 4 10	0 5 11 14
	13	3 6 10 14	0 2 7 8
	16	0 3 5 9	4 6 7 14
	20	0 2 6 13	4 5 7 10
	22	8 9 10 14	0 3 4 12
	23	0 4 13 14	1 6 9 12
	24	0 7 9 12	1 2 5 13
	25	0 1 4 11	3 5 7 13
	28	8 11 12 13	0 2 9 14

p	N	$\pm x$	$\pm x'$
37	1	0 2 8 10 11	1 7 14 16 18
	3	6 11 12 15 18	0 2 7 9 17
	4	1 2 5 9 14	0 4 15 16 17
	7	0 2 12 16 18	4 9 11 14 15
	9	0 4 6 7 13	3 5 11 16 17
	10	0 1 10 14 15	3 6 9 11 13
	11	2 7 11 13 14	0 1 6 8 9
	12	0 3 4 14 18	1 7 12 13 15
	16	0 3 5 7 8	2 4 9 10 18
	21	3 12 13 14 17	0 5 7 11 18
	25	2 4 5 6 18	0 3 10 13 18
	26	0 1 6 11 17	4 5 8 10 12
	27	1 4 8 17 18	0 6 10 14 16
	28	7 8 9 15 18	0 1 4 5 13
	30	8 10 13 16 17	0 2 3 12 15
	33	0 9 13 15 16	6 7 10 12 17
	34	0 5 9 12 17	1 2 3 8 16
	36	3 5 6 10 15	0 8 11 12 14

p	N	$\pm x$							$\pm x'$						
41	1			12	13	14	16	18		0	1	3	9	17	19
	2		0	2	5	10	11	17			1	8	15	16	19
	4			5	9	13	15	17		0	2	3	6	7	18
	5		0	1	2	6	13	16			3	5	8	12	18
	8		0	4	7	10	19	20			2	3	9	11	16
	9		0	3	9	10	14	16			1	2	5	7	13
	10			1	3	10	13	19		0	7	15	16	17	20
	16			7	10	11	15	18		0	4	5	6	12	14
	18			3	4	7	16	17		0	6	8	10	11	15
	20		0	2	4	9	12	15			5	6	10	16	17
	21		0	1	5	12	15	18			4	8	11	13	20
	23			5	11	14	19	20		0	8	10	12	13	17
	25			2	8	12	17	19		0	3	4	5	13	15
	31			6	7	8	9	14		0	11	12	16	19	20
	32		0	1	3	8	14	20			4	6	9	18	19
	33		0	5	7	8	16	19			1	14	17	18	20
	36		0	6	9	13	18	20			2	4	10	14	15
	37			1	4	6	11	12		0	2	13	14	18	19
	39		0	4	8	11	17	18			7	9	10	12	20
	40			2	3	6	15	20		0	1	7	9	11	14
53	1	0	5	8	10	12	14	16	1	4	13	19	20	21	22
	4	2	8	9	11	13	15	26	0	10	16	20	21	24	25
	6	7	11	18	19	22	24	25	0	4	13	15	16	21	23
	7	6	7	15	16	18	21	22	0	1	4	8	10	17	19
	9	3	4	7	10	12	13	14	0	5	11	15	17	23	24
	10	0	2	3	4	12	23	24	1	5	8	10	13	18	21
	11	1	2	7	8	9	17	21	0	6	10	11	13	22	26
	13	0	2	9	14	21	22	25	3	7	12	15	17	18	20
	15	0	2	4	5	16	17	26	3	8	9	11	18	19	23
	16	0	3	5	11	13	20	21	1	4	16	18	22	23	26
	17	4	8	15	17	21	22	25	0	1	2	9	13	18	24
	24	0	7	8	11	21	23	26	3	5	9	14	15	17	22
	25	1	4	5	6	11	12	20	0	3	7	13	17	25	26
	28	0	2	8	15	16	19	20	9	11	12	14	17	21	23
	29	4	5	9	16	20	24	26	0	1	2	6	12	15	25
	36	0	5	7	10	19	22	23	6	8	14	20	24	25	26
	37	1	3	10	14	15	23	24	0	6	9	12	16	17	19
	38	1	3	5	12	13	16	25	0	7	9	10	14	15	20
	40	2	10	11	16	17	20	26	0	4	5	6	7	8	24
	42	0	12	15	18	19	21	24	2	5	6	7	20	23	25
	43	6	9	10	18	19	23	25	0	1	7	11	14	16	22
	44	0	1	9	12	20	22	26	2	4	11	14	16	18	19
	46	0	13	14	18	20	23	25	2	3	6	10	21	24	26
	47	0	1	3	6	14	19	26	2	8	10	12	13	22	24
	49	0	3	6	8	17	18	22	5	7	12	15	19	25	26
	52	6	9	13	14	19	23	24	0	3	4	11	17	18	25

p	N	$\pm x$								$\pm x'$							
61	1	0	2	4	13	14	15	21	26	1	7	9	22	25	27	29	30
	3	4	5	7	8	11	12	17	28	0	2	10	15	16	18	25	29
	4	1	2	3	7	11	14	17	18	0	4	8	9	19	26	28	30
	5	1	10	13	21	22	23	26	30	0	2	3	5	9	18	24	28
	9	0	2	6	12	16	17	19	22	3	5	14	20	21	26	27	29
	12	0	3	4	11	20	25	29	30	5	8	10	14	16	22	24	27
	13	0	1	2	5	11	13	27	28	3	4	7	12	14	16	21	24
	14	1	6	18	20	21	24	25	26	0	3	10	11	14	19	23	29
	15	0	9	11	16	20	21	22	24	1	4	7	8	15	18	19	25
	16	0	1	5	8	9	16	18	23	2	4	6	14	22	25	27	28
	19	2	4	9	18	21	23	27	30	0	8	10	11	12	20	25	26
	20	0	4	5	6	10	13	18	25	1	2	9	15	17	19	20	26
	22	0	3	7	8	13	15	24	27	5	6	12	14	18	19	20	23
	25	0	4	8	9	10	14	17	20	3	5	12	13	16	23	26	28
	27	10	12	15	21	23	24	25	28	0	6	7	13	14	16	26	30
	34	0	5	7	16	19	21	25	29	3	9	10	12	13	18	20	30
	36	3	6	7	9	10	19	21	28	0	4	12	17	23	24	27	29
	39	5	6	9	10	15	24	26	29	0	8	16	18	20	21	27	28
	41	4	11	18	19	22	23	24	26	0	5	6	12	15	17	21	30
	42	0	1	10	12	19	24	27	30	8	9	13	15	17	22	23	25
	45	2	3	5	8	17	22	29	30	0	6	7	9	11	15	23	27
	46	11	15	16	17	18	26	27	30	0	1	2	7	13	20	23	24
	47	0	1	9	12	14	26	28	29	5	11	13	15	19	20	24	30
	48	7	10	13	16	17	20	28	29	0	1	3	6	8	11	21	22
	49	2	6	7	8	12	20	27	29	0	1	14	17	24	25	28	30
	52	6	8	13	14	19	24	28	29	0	2	4	5	7	10	22	26
	56	0	3	6	15	20	22	23	28	2	9	11	12	13	19	21	25
	57	0	3	17	19	23	25	26	27	1	4	11	15	16	22	28	29
	58	0	7	12	14	15	18	22	30	1	3	4	6	10	16	17	27
	60	2	8	11	14	16	23	25	30	0	13	17	18	19	21	22	29

8. On pourrait faire une étude sur la répartition des nombres $0, 1, 2, 3, \ldots, \frac{p-1}{2}$ dans les tables que nous venons de dresser.

On remarquera, par exemple, que dans le cas de $\left(\frac{N}{p}\right) = -1$, 0 figure dans la table si $p \equiv 3$ (Mod. 4) et n'y figure pas si $p \equiv 1$ (Mod. 4). Les autres nombres interviennent le même nombre de fois $\left[\frac{p-3}{4}\right.$ fois si $p \equiv 3$ (Mod. 4) et $\left.\frac{p-1}{4}\right.$ fois si $p \equiv 1$ (Mode 4)$\Big]$.

Si $\left(\frac{N}{p}\right) = +1$ et $p \equiv 3$ (Mod. 4), le signe de x est précis et chaque nombre $1, 2, 3, \ldots, p-1$ intervient $\dfrac{\frac{p+1}{4} \cdot \frac{p-1}{2}}{p-1} = \frac{p+1}{8}$ fois, si le module est de la forme $8k+7$.

Mais si le module est de la forme $8k+3$, les résidus interviennent $\frac{p+5}{8}$ fois et les non résidus $\frac{p-3}{8}$ fois.

Si le module est de la forme $4k+1$ et $\left(\frac{N}{p}\right)=+1$, 0 intervient dans la table de x, ou dans la table de x', suivant que $\left(\frac{N}{p}\right)_4=+1$ ou $\left(\frac{N}{p}\right)_4=-1$.

Les autres nombres 1, 2, 3, ..., $\frac{p-1}{2}$ interviennent $\frac{p-1}{4}$ fois dans la table de valeur de x ou x'.

Ces nombres interviennent $\frac{p-1}{8}$ fois dans la table des valeurs de x ou x', si le module est de la forme $8k+1$.

Enfin, les résidus interviennent $\frac{p+3}{8}$ fois et les non résidus $\frac{p-5}{8}$ fois dans les valeurs de x', si le module est de la forme $8k+5$.

9. Nous signalerons encore la réduction qui se présente pour certains nombres d'une forme spéciale.

Si N est un diviseur de $a^n \pm b^n$ et si p est un nombre premier impair qui divise n, chaque facteur de N est de la forme $kp+1$. On aura donc (Mod. p)

$$x+y \equiv 1,$$

$$x-y \equiv 1,$$

ce qui donne $\quad x \equiv 1$ (Mod. p), $\quad y \equiv 0$ (Mod. p).

Mais $y \equiv 0$ (Mod. p), donne $y^2 \equiv 0$ (Mod. p^2) et l'équation $x^2 - y^2 = N$ devient (Mod. p^2)

$$x^2 \equiv N \text{ (Mod. } p^2).$$

Cette congruence admet en général deux racines

$$x \equiv \pm z \text{ (Mod. } p^2).$$

Mais une seule de ces racines est compatible avec la solution trouvée précédemment $x \equiv 1$ (Mod. p). On aura une seule solution de x (Mod. p^2).

Une réduction analogue se présente dans la factorisation des termes des séries récurrentes de second degré.

On ne négligera pas l'avantage de n'avoir qu'une seule valeur de x (Mod. p^2), au lieu de $\frac{p+1}{2}$ valeurs de x (Mod. p), comme cela arrive dans le cas général.

10. Examinons enfin le module 2^n.

Soit d'abord $N \equiv 3$ (Mod. 4). Alors, l'équation $x^2 - y^2 = N$, exige que x soit pair et y impair. Les solutions ainsi trouvées seront donc irréductibles.

Si $N \equiv 3$ (Mod. 8), on aura $x \equiv 2$ (Mod. 4),

7 (Mod. 8), 0 (Mod. 4),

ou $x \equiv \sqrt{N+1}$ (Mod. 8).

Tant qu'on ne connaît rien sur le nombre N à factoriser, ces solutions sont irréductibles, mais un renseignement supplémentaire sur le nombre N permet de pousser plus loin la limitation des valeurs de x.

Soit $N \equiv 3$ (Mod. 8), cas qu'on peut subdiviser en deux, en le développant suivant le module 16.

$$\left.\begin{array}{l} \text{Si} \quad N \equiv 3 \text{ (Mod. 16)} \\ \qquad\quad 11 \end{array}\right\} \text{ on aura } \quad x \equiv \pm 2 \text{ (Mod. 8)}.$$

Si on parvient à établir la nature du nombre -2 pour le module N, c'est-à-dire, si on sait que $\left(\frac{-2}{N}\right) = +1$, les facteurs $x \pm y$ de N, doivent être de la forme $8k+1$, ou 3 et on aura

Si $N \equiv 3$ (Mod. 16), $x \equiv +2$ (Mod. 8),

$N \equiv 11$ (Mod. 16), $x \equiv +6$ (Mod. 8).

Si de même $N \equiv 7$ (Mod. 8), il y a lieu de s'assurer si 2 est résidu, ou non de N.

Si $\left(\frac{2}{N}\right) = +1$, on aura

$N \equiv 7$ (Mod. 16), $x \equiv 4$ (Mod. 8),

15 0

Soit ensuite $N \equiv 5$ (Mod. 8), cas qu'on subdivisera en quatre autres, suivant le module 32.

Si $N \equiv 5, \quad 13, \quad 21, \quad 29$ (Mod. 32),

on aura $\pm x \equiv 3, \quad 7, \quad 5, \quad 1$ (Mod. 16),

ou si on veut $x \equiv \sqrt{N+4}$ (Mod. 32).

Dans ce cas, y est divisible par deux, sans l'être par quatre, $y \equiv 2$ (Mod. 4).

Si, de plus, on sait que $\left(\frac{-1}{N}\right) = +1$, on aura

pour $\quad N \equiv 4, \quad 13, \quad 21, \quad 29$ (Mod. 32),

$\quad x = 3, \quad 7, \quad 11, \quad 15$ (Mod. 16),

soit *une* solution (Mod. 16), au lieu de *deux*, comme dans le cas général.

11. Supposons enfin, qu'on ait $N \equiv 1$ (Mod. 8), Alors $y \equiv 0$ (Mod. 4) et il y aura lieu de s'assurer si l'un des nombres -1, ± 2 est résidu de N.

On peut, à priori, trouver la forme des solutions de x.

En effet, on peut avoir $y \equiv 4$ (Mod. 8), alors $y^2 \equiv 16$ (Mod. 128), car tout carré impair est de la forme $8k+1$, on aura donc $y^2 \equiv 16.(8k+1) \equiv 16$ (Mod. 128), d'où $x \equiv \pm \sqrt{N+16}$ (Mod. 128), ou $\pm r_1$ (Mod. 64).

On peut aussi avoir $y \equiv 8$ (Mod. 16), alors

$y^2 \equiv 64$ (Mod. 2^9), et $x \equiv \pm \sqrt{N+64}$ (Mod. 2^9) ou $\pm r_2$ (Mod. 2^8).

On peut ensuite avoir $y \equiv 16$ (Mod. 2^5), ce qui donne

$y^2 \equiv 2^8$ (Mod. 2^{11}), d'où $x \equiv \pm \sqrt{N+2^8}$ (Mod. 2^{11}) $\equiv \pm r_3$ (Mod. 2^{10}).

On peut encore avoir $y \equiv 2^5$ (Mod. 2^6), donnant $y^2 \equiv 2^{10}$ (Mod. 2^{13}), d'où $x \equiv \pm \sqrt{N+2^{10}}$ (Mod. 2^{13}) $\equiv \pm r_4$ (Mod. 2^{12}), ...

On aura ainsi

$\pm x \equiv z_1$ (Mod. 2^6), z_2 (Mod. 2^8), z_3 (Mod. 2^{10}), ..., z_k (Mod. 2^{2k+4}).

A ces solutions correspond une valeur de $y = 2^e.i$ (i impair)

$$f \equiv 2, \quad 3, \quad 4, \quad \ldots, \quad k.$$

On peut, dans certains cas, expliciter la valeur $\sqrt{N+2^{2k}}$ trouvée précédemment pour x.

Soit, pour fixer les idées, la valeur de $x = \sqrt{N + 2^{2k}}$ (Mod. 2^{2k+3}), pour $N \equiv 1$ (Mod. 2^a), a étant suffisamment élevé. On trouve

$$\sqrt{N + 2^4} \text{ (Mod. } 2^7) \equiv \pm 23 \text{ (Mod. } 2^6).$$

$\sqrt{N + 2^6}$	2^9	33	2^8
$\sqrt{N + 2^8}$	2^{11}	129	2^{10}
$\sqrt{N + 2^{10}}$	2^{13}	513	2^{12}
$\sqrt{N + 2^{12}}$	2^{15}	2049	2^{14}
. . . . .			
$\sqrt{N + 2^{2k}}$	2^{2k+3}	$2^{2k-1} + 1$	2^{2k+2}.

On suppose $a \geqslant 2k + 3$.

A chaque valeur de x correspond une forme particulière de la décomposition $(x + y)(x - y)$.

Ainsi, si

$x = \sqrt{N + 16}$, on aura $y \equiv 4$ et $N \equiv 3 \times 3$ ou 5×5 (Mod. 8),

$\sqrt{N + 64}$,	8	7×7	9×9	16
$\sqrt{N + 2^8}$,	16	15×15	17×17	32

etc.

12. Telles sont les réductions, tant qu'on ne connaît rien sur le nombre N. Mais le nombre N étant $\equiv +1$ (Mod. 8), les nombres -1, ± 2, peuvent en être des résidus.

La connaissance d'un résidu est très utile et diminue le nombre des valeurs admissibles.

Ainsi, si (-1) est résidu de N, les deux facteurs de N, $x + y$ et $x - y$, sont de la forme $4k + 1$, et il en est de même de x, et on aura, si $N \equiv 1$ (Mod. 2^a)

$$x \equiv +41 \text{ (Mod. } 64), \quad +33 \text{ (Mod. } 256), \quad +129 \text{ (Mod. } 2^{10}), \text{ etc.}$$
$$+ (2^{2k-1} + 1) \text{ (Mod. } 2^{2k+2}).$$

Si on connaît le résidu $+2$, les deux facteurs sont de la forme $8k \pm 1$, et les solutions sont les mêmes que dans le cas général, sauf que la valeur $x \equiv \sqrt{N+16}$ (Mod. 128), (conduisant aux facteurs de la forme $8k \pm 3$), est inadmissible.

On aura dans ce cas, deux valeurs sur 256, deux valeurs sur 2^{10}, etc., soit à la limite, un cas sur 96 à étudier.

Enfin, si on sait que -2 est résidu de N, on aura en supposant $N \equiv 1$ (Mod. 2^a)

$$x \equiv +23 \text{ (Mod. } 64), \quad +33 \text{ (Mod. } 256), \quad +129 \text{ (Mod. } 2^{10}), \text{ etc.,}$$
$$+(2^{2k-1}+1) \text{ (Mod. } 2^{2k+2}).$$

Remarquons enfin, que deux des résidus (-1), $+2$ et (-2), entraînent le troisième et alors pour $N \equiv 1$ (Mod. 2^a)

$$x \equiv +33 \text{ (Mod. } 256), \quad +129 \text{ (Mod. } 2^{10}), \quad \ldots,$$
$$+(2^{2k-1}+1) \text{ (Mod. } 2^{2k-2}).$$

Nous remarquerons que dans le cas de $N \equiv 1$ (Mod. 8), à chaque valeur de x correspondent des facteurs d'une certaine forme. Voici les facteurs correspondant aux valeurs de x dans le cas de $N \equiv 1$ (Mod. 2^a)

$x \equiv +23$	(Mod. 64),	$N \equiv 3 \times 3$	(Mod. 8),
$+41$	64	5×5	8
33	256	9×9	16
223	256	7×7	16
129	1024	17×17	32
895	1024	15×15	32
513	4096	33×33	64
3583	4096	31×31	64
2049	16384	65×65	128
14335	16384	63×63	128
8193	2^{16}	129×129	2^8
57343	2^{16}	127×127	2^8
etc.,		etc.,	
$2^{2k-3}+1$	2^{2k}	$(2^{k-1}+1)(2^{k-1}+1)$	2^k
$7.2^{2k-3}-1$	2^{2k}	$(2^{k-1}-1)(2^{k-1}-1)$	2^k

13. Dans certains cas, on aura une source supplémentaire de réduction (Mod. 2^n). Par exemple, quand on sait que chaque facteur est d'une certaine forme (Mod. 2^n), on aura $y \equiv 0$ (Mod. 2^k), ce qui exige que x soit d'une forme spéciale, choisie parmi celles qui sont admissibles dans le cas général.

Soit N facteur de $a^k \pm b^k$ et 2^n un facteur de k, on aura

$$x + y \equiv 1 \text{ (Mod. } 2^n),$$

$$x - y \equiv 1 \quad \text{»}$$

d'où $\quad x \equiv 1$ (Mod. 2^{n-1}), $\quad y \equiv 0$ (Mod. 2^{n-1}),

$$y^2 \equiv 0 \text{ (Mod. } 2^{2n-2}), \quad \text{d'où} \quad x^2 \equiv \text{N (Mod. } 2^{2n-2}),$$

cette congruence donne $x \equiv z$ (Mod. 2^{2n-3}).

Elle a deux solutions, dont une seule est compatible avec la condition $x \equiv 1$ (Mod. 2^{n-1}).

Par exemple, $\text{N} = 2^{128} + 1$, admet des facteurs de la forme

$$512k + 1, \quad \text{d'où} \quad x + y \equiv 1 \text{ (Mod. } 512),$$

$$x - y \equiv 1 \qquad 512$$

$$x \equiv 1, \qquad y \equiv 0 \text{ (Mod. } 256),$$

$$y^2 \equiv 0 \text{ (Mod. } 256^2), \qquad x^2 \equiv 1 \text{ (Mod. } 2^{16}),$$

d'où $\quad x \equiv +1$ (Mod. 2^{15}).

On peut même établir qu'on aura $y \equiv 0$ (Mod. 512) (1), par conséquent $x \equiv +1$ (Mod. 2^{17}).

On aura ainsi

$$x \equiv +2^{17} + 1 \text{ (Mod. } 2^{20}),$$

si les deux facteurs sont

$$(2^9 + 1) \times (2^9 + 1) \text{ (Mod. } 2^{10}),$$

et $\quad x \equiv +2^{19} + 1$ (Mod. 2^{22}),

si les deux facteurs sont

$$(2^{10} + 1) \times (2^{10} + 1) \text{ (Mod. } 2^{11}),$$

---

(1) Si on pose $x + y = 512k + 1$, $x - y = 512l + 1$, on trouve $y = 256\,(k - l)$, on trouve ensuite que $k + l$ (ainsi que $k - l$) est pair, donc $y \equiv 0$ (Mod. 512).

De même $$x \equiv 2^{21} + 1 \text{ (Mod. } 2^{24}),$$

si les deux facteurs sont

$$(2^{11} + 1) \times (2^{11} + 1) \text{ (Mod. } 2^{12}),$$

etc.,

et, en général $$x \equiv 2^{2k+1} + 1 \text{ (Mod. } 2^{2k+4}),$$

si les deux facteurs sont

$$(2^{2k+1} + 1) \times (2^{2k+1} + 1) \text{ (Mod. } 2^{2k+2}).$$

Cela revient à commencer l'énumération des solutions de x

$$x = \sqrt{N + 2^{2k}} \text{ (Mod. } 2^{2k+3}), \qquad \text{ou} \qquad \pm r_k \text{ (Mod. } 2^{2k+2}),$$

à partir d'une certaine valeur de k. Ainsi, dans le cas de $N = 2^{128} + 1$, on commencera cette énumération à partir de $k = 9$. En outre, à cause de $x \equiv 1$ (Mod. 512), le signe de r_k est précis.

14. Ainsi qu'on a pu le constater dans ce qui précède, on peut toujours mettre à profit la connaissance d'un résidu -1, $+2$ ou -2.

Pour ce qui est des résidus impairs $\pm p$ ($p \geqslant 3$), on peut profiter de la connaissance d'un résidu $\pm p$ dans les cas suivants

$$\left(\frac{-p}{N}\right) = +1, \qquad \text{si} \qquad p \equiv 3 \text{ (Mod. } 4),$$

et $$\left(\frac{+p}{N}\right) = +1, \qquad \text{si} \qquad p \equiv 1 \text{ (Mod. } 4).$$

Peut-on profiter d'un *renseignement négatif* ?

Nous entendons par *renseignement négatif*, la connaissance qu'un nombre $-p$. est non résidu de N, si $p \equiv 3$ (Mod. 4), ou qu'un nombre p est non résidu de N, si $p \equiv 1$ (Mod. 4)

Il est facile de voir, que ce renseignement est inutilisable, si le nombre N peut contenir plus de deux facteurs, car $\pm p$ étant non résidu de N, le nombre N peut être le produit de trois non résidus ou d'un non résidu et de deux résidus.

Mais, si le nombre N ne contient pas plus de deux facteurs, un renseignement négatif, peut être utilisé.

Soit, pour fixer les idées $p = 11$, $N \equiv 3$.

On aura $\pm x \equiv 1, 2, 5$, si on ne connaît pas le symbole $\left(\frac{-11}{N}\right)$.

On aura $+ x \equiv 1, 2, 5$,

si $\left(\frac{-11}{N}\right) = +1$. Enfin, on aura $x \equiv 6, 9, 10$,

si $\left(\frac{-11}{N}\right) = -1$ et si N ne contient pas plus de deux facteurs.

Soit encore $N \equiv 4$ (Mod. $p = 13$).

On aura $\pm x \equiv 0, 1, 2, 4$, si on ne connaît pas le symbole $\left(\frac{13}{N}\right)$.

On aura

$$\pm x \equiv 0, 4, \qquad \text{si} \qquad \left(\frac{13}{N}\right) = +1,$$

$$\pm x \equiv 1, 2, \qquad \text{si} \qquad \left(\frac{13}{N}\right) = -1,$$

et si N ne contient pas plus de deux facteurs.

On notera qu'un renseignement positif peut être utilisé, quel que soit le nombre de facteurs composant N, mais un renseignement negatif ne peut l'être, que si le nombre de facteurs de N est tout au plus deux.

CHAPITRE XIII.

De l'équation $x^2 + Dy^2 = N$.

1. Nous considérerons dans ce chapitre cette équation, sous un autre point de vue, que celui que nous avons examiné pp. 113-120 dans l'étude des formes.

Cette fois-ci, il s'agit d'un nombre N à factoriser.

Nous rappellerons que si le nombre N peut être mis sous la forme $N = x^2 + Dy^2$, le nombre $-D$ est résidu de N (T, I, p. 98). La réciproque n'est pas vraie.

Toutefois, on peut énoncer la proposition suivante qui tient lieu de la réciproque.

Si $-D$ est résidu de N, le nombre N peut être représenté par une des formes réduites du déterminant $-D$.

2. L'équation $N = x^2 + Dy^2$ contient deux inconnues, dont une doit être déterminée par tâtonnement, l'autre pouvant alors être calculée directement.

D'une façon générale, il est préférable de déterminer x par tâtonnement.

Si, par exemple $D > 1$, on aura pour déterminer x la congruence $N \equiv x^2$ (Mod. D), qui déterminera deux valeurs de x (Mod. D), si D est premier et 2^n valeurs de x (Mod. D), si D contient n facteurs inégaux. Ainsi, on aura à chercher x parmi les $\frac{2^n \cdot \sqrt{N}}{D}$ valeurs possibles. Pour déterminer y, on aura à considérer toutes les $\sqrt{\frac{N}{D}}$ valeurs éventuelles de y.

Nous verrons, de plus, qu'on peut construire d'avance des tables donnant la valeur (Mod. p) de x, mais il serait plus compliqué de construire de telles tables pour les valeurs éventuelles de y (T, I, Table, p. 187-204).

Enfin, les modules premiers qui entrent comme facteurs dans D peuvent être avantageusement employés pour limiter les valeurs de x, mais ne peuvent pas l'être pour celles de y.

3. Si $D > 0$, les limites de x sont

$$0 < x < \sqrt{N},$$

et celles de y

$$0 < x < \sqrt{\frac{N}{D}}.$$

Mais, si $D < 0$, on ne peut trouver qu'une seule limite de x, $x > \sqrt{N}$. Toutefois, dans le cas de $D = -1$, on trouve une limite supérieure de x, $x < \frac{N+1}{2}$.

On peut même serrer davantage les limites et prendre

$$\sqrt{N} < x < \frac{1}{2}\left(a + \frac{N}{a}\right),$$

quand on sait que N doit posséder un facteur entre a et $\sqrt{N}$ ($a < \sqrt{N}$) (T, I, p. 144).

Si $D < 0$ et si l'équation $x^2 - Dy^2 = N$ est possible, elle l'est d'une infinité de manières, sauf quand D est un carré parfait.

4. Considérons l'équation $x^2 - Dy^2 = \pm N$.

Soit a et b une solution particulière de cette équation et α et β les deux plus petits nombres vérifiant l'équation

$$\alpha^2 - D\beta^2 = +1, \qquad (\alpha > 1, \qquad \beta \neq 0). \tag{1}$$

Si on multiplie les équations

$$a^2 - Db^2 = \pm N,$$

$$\alpha^2 - D\beta^2 = 1,$$

on trouve

$$(a\alpha - Db\beta)^2 - D(a\beta - b\alpha)^2 = \pm N,$$

de sorte qu'on peut poser

$$\begin{aligned} x &= \pm(a\alpha - Db\beta), \\ y &= \pm(a\beta - b\alpha). \end{aligned} \tag{2}$$

Ainsi, de chaque solution (a, b), on déduit une nouvelle solution (x, y) par les formules (2).

Notons que $\alpha > 1$ et que dans (2) les signes seront choisis de façon à rendre x et y positifs.

Afin de déterminer le signe à prendre pour que x et y soient > 0, nous examinerons avec TCHEBICHEFF [1], séparément les deux cas.

5. Soit d'abord l'équation $x^2 - Dy^2 = + N$.

Puisqu'on a
$$a^2 - Db^2 = + N,$$
$$\alpha^2 - D\beta^2 = 1,$$
$$x = \pm (a\alpha - Db\beta),$$
on aura en éliminant a et α
$$x = \pm (\sqrt{Db^2 + N} \cdot \sqrt{D\beta^2 + 1} - Db\beta),$$
expression positive, si on la prend avec le signe $+$.

On aura donc $\quad x = + (a\alpha - Db\beta).$

Voyons maintenant, dans quel cas la nouvelle solution est plus petite que celle dont on est parti.

Pour avoir
$$x < a \quad \text{ou} \quad a\alpha - Db\beta < a,$$
on doit avoir
$$Db\beta > a(\alpha - 1),$$
ou
$$D^2 b^2 \beta^2 > a^2 (\alpha - 1)^2,$$
ou en éliminant b et β
$$D^2 \cdot \frac{a^2 - N}{D} \cdot \frac{\alpha^2 - 1}{D} > a^2 (\alpha - 1)^2,$$
ou $\quad (a^2 - N)(\alpha + 1) > a^2 (\alpha - 1) \quad$ puisque $\quad \alpha > 1,$

ou
$$a > \sqrt{\frac{\alpha + 1}{2} N}.$$

Ainsi, si $a > \sqrt{\frac{\alpha + 1}{2} N}$, on peut déduire d'une solution (a, b) une nouvelle solution (x, y) dans laquelle $x < a$.

Il en résulte qu'on trouvera finalement une solution (a, b) avec $a < \sqrt{\frac{\alpha + 1}{2} N}$, si, bien entendu, l'équation $x^2 - Dy^2 = N$ est possible.

Puisque a et b croissent simultanément, on aura $b < \sqrt{\frac{\alpha - 1}{2D} N}$.

---

(1) Journal de Liouville, 1851, p. 257-282.
TCHEBICHEFF. Œuvres I, p. 73.

6. Soit, en deuxième lieu, l'équation $x^2 - Dy^2 = -N$.

On trouve

$$y = \pm (a\beta - b\alpha) = \pm (\beta \sqrt{Db^2 - N} - b \sqrt{D\beta^2 + 1})$$

$$= \pm \frac{-N\beta^2 - b^2}{\beta \sqrt{Db^2 - N} + b \sqrt{D\beta^2 + 1}}.$$

La valeur de y sera positive, si on la prend avec le signe —, on aura donc

$$y = -(a\beta - b\alpha).$$

Pour que la nouvelle solution (xy) soit plus petite que celle dont on est parti, il faut qu'on ait

$$-a\beta + b\alpha < b,$$

ou

$$b(\alpha - 1) < a\beta, \qquad \text{ou} \qquad b^2(\alpha - 1)^2 < a^2\beta^2,$$

ou

$$b^2(\alpha - 1)^2 < \frac{(Db^2 - N)(\alpha^2 - 1)}{D}, \qquad \text{ou puisque} \qquad \alpha > 1,$$

$$Db^2(\alpha - 1) < (Db^2 - N)(\alpha + 1),$$

d'où

$$b > \sqrt{\frac{\alpha + 1}{2D} N}.$$

Ainsi, si $b > \sqrt{\frac{\alpha + 1}{2D} N}$, on peut trouver une solution (x, y) en partant d'une solution (a, b). La nouvelle solution sera plus simple que celle dont on est parti.

Il en résulte, que si l'équation $x^2 - Dy^2 = -N$ est possible, on trouvera une solution $x = a$, $y = b$ et telle que

$$b < \sqrt{\frac{\alpha + 1}{2D} N}.$$

A cette limite de b correspond une limite $a < \sqrt{\frac{\alpha - 1}{2} N}$.

7. Les solutions qui satisfont aux conditions des limites trouvées plus haut, à savoir, les solutions

$$x = a, \qquad y = b, \qquad \text{de l'équation} \qquad x^2 - Dy^2 = +N,$$

avec

$$a < \sqrt{\frac{\alpha + 1}{2} N}, \qquad b < \sqrt{\frac{\alpha - 1}{2D} N}, \tag{3}$$

ou bien les solutions

$$x = a, \qquad y = b, \qquad \text{de l'équation} \qquad x^2 - Dy^2 = -N,$$

avec

$$a < \sqrt{\frac{\alpha - 1}{2} N}, \qquad b < \sqrt{\frac{\alpha + 1}{2D} N}, \tag{4}$$

seront dites solutions *primitives*.

Toute autre solution de l'équation $x^2 - Dy^2 = \pm N$ sera une solution *dérivée*.

8. L'équation $x^2 + y^2 = N$ mérite une mention spéciale, tout aussi bien à cause de son importance que de sa forme particulière.

Cette équation étant symétrique en x et y, il en résulte que les inconnues sont interchangeables.

D'abord, au point de vue des limites, l'un des carrés doit être compris entre 0 et $\frac{N}{2}$, l'autre entre $\frac{N}{2}$ et N.

Il suit de là qu'on aura pour l'une des inconnues x ou y

$$0 < x \qquad \text{ou} \qquad y < \sqrt{\frac{N}{2}}, \tag{1}$$

$$\sqrt{\frac{N}{2}} < y \qquad \text{ou} \qquad x < \sqrt{N}. \tag{2}$$

Or, les limites (2) sont bien plus rapprochées l'une de l'autre que (1), car

$$\sqrt{N} - \sqrt{\frac{N}{2}} = \sqrt{\frac{N}{2}}(\sqrt{2} - 1) = 0, \qquad 4142136 \ldots \sqrt{\frac{N}{2}}.$$

Ensuite, l'une des inconnues devant être paire, l'autre impaire (on suppose que N est impair), on peut prendre

$$x = \text{pair} \quad \text{ou} \quad \text{impair},$$

$$y = \text{impair} \quad \text{ou} \quad \text{pair}.$$

Mais, on ne peut pas prendre simultanément pour l'une des inconnues les limites données (0 et $\sqrt{\frac{N}{2}}$ ou $\sqrt{\frac{N}{2}}$ et $\sqrt{N}$) et fixer sa parité.

Il est préférable de fixer la parité de x, quitte à sacrifier l'avantage résultant des limites plus rapprochées.

Nous supposerons que x est impair.

9. Dans certains cas, on peut trouver une solution directe de l'équation $x^2 + Dy^2 = N$.

Considérons d'abord le cas de $D = 1$ et quand N est premier.

Posons $N = 4k + 1$ (autrement l'équation $x^2 + y^2 = N$ ne serait pas possible).

Si on connaît une racine primitive ρ de N, on aura $\rho^{2k} \equiv -1$ (Mod. N), soit $\rho^k \equiv a$ (Mod. N), on aura donc $a^2 \equiv -1$ (Mod. N).

Considérons la fraction $\frac{a}{N}$ et formons les réduites de cette fraction. La dernière de ces réduites est $\frac{a}{N}$.

Les derniers dénominateurs de deux réduites consécutives qui ne surpassent pas $\sqrt{N}$ donnent les valeurs de x et y (R, 51 et 269, T. I, p. 99).

Ce procédé s'applique encore quand $D = 2$ ou 3 et quand on connaît la solution de la congruence $x^2 \equiv -2$ ou $x^2 \equiv -3$ (Mod. N).

Si on ne connaît pas une racine primitive de N, il suffit de prendre un non résidu n quelconque de N.

En effet, n étant un non résidu, on aura $n^{2k} \equiv -1$.

Si on a plusieurs représentations de N de la forme

$$N = x^2 + D_i\, y^2,$$

telles que le produit de certains $(-D_i)$ conduit à $(-D)$ à un facteur carré près, on peut encore trouver la solution directe comme suit :

Soit, pour fixer les idées, $Dn^2 = D_1D_2D_3$, $x^2 + Dy^2 = N$ l'équation donnée et

$$N = a^2 + D_1b^2 = c^2 + D_2d^2 = e^2 + D_3f^2.$$

Si on multiplie membre à membre, les congruences

$$a^2 \equiv -D_1b^2 \text{ (Mod. N)},$$

$$c^2 \equiv -D_2d^2,$$

$$e^2 \equiv -D_3f^2,$$

on trouve

$$(ace)^2 \equiv -\mathrm{D}n^2 (bdf)^2 \text{ (Mod. N)},$$

$$k^2 + \mathrm{D}l^2 \equiv 0 \text{ (Mod. N)}.$$

Si donc la représentation $\mathrm{N} = x^2 + \mathrm{D}y^2$ est possible, on peut poser

$$k^2 + \mathrm{D}l^2 = \mathrm{N.Q}.$$

Supposons que Q puisse lui-même être mis sous la forme, $u^2 + \mathrm{D}v^2$, on aura alors

$$k^2 + \mathrm{D}l^2 = (x^2 + \mathrm{D}y^2)(u^2 + \mathrm{D}v^2) = (xu \pm \mathrm{D}yv)^2 + \mathrm{D}(xv \mp yu)^2.$$

On peut alors poser

$$xu \pm \mathrm{D}yv = k,$$

$$xv \mp yu = l,$$

d'où on déterminera x et y.

Ce procédé est surtout applicable, quand D est un des nombres d'Euler (T. II, p. 119).

Si $\mathrm{D} = 1$, 2 ou 3 et qu'on ait $\mathrm{D}n^2 = \mathrm{D}_1\mathrm{D}_2\mathrm{D}_3 \ldots$, on aura comme précédemment $k^2 + \mathrm{D}l^2 \equiv 0$ (Mod. N); en multipliant par l'associé l' de l (Mod. N), il viendra $k^2l'^2 + \mathrm{D} \equiv 0$ et on déterminera facilement x et y par les dénominateurs des réduites des fractions continues de $\frac{kl'}{\mathrm{N}}$.

Remarquons encore que si $\mathrm{D} = 1$, on peut résoudre l'équation $x^2 + y^2 = \mathrm{N}$ par le développement de $\sqrt{\mathrm{N}}$ en fraction continue.

Si la partie symétrique de la période contient $2k$ termes, on aura

$$x_k = \frac{\sqrt{\mathrm{N}} + \mathrm{N}_k}{\mathrm{D}_k} = a_{k+1} + \frac{1}{x_{k+1}},$$

donnant

$$\mathrm{N} = \mathrm{N}_k^2 + \mathrm{D}_k^2 \text{ (T. II, 17)}.$$

Toutefois, si N est quelque peu grand, le procédé devient fastidieux, bien que cette solution soit directe.

Signalons encore la solution suivante, plus élégante que pratique.

Si $\mathrm{N} = 4n + 1$ est un nombre premier, posons

$$q = n! \qquad r = (2n)! : (n!),$$

et posons

$$\pm x \equiv r : (2q), \qquad \pm y \equiv \frac{1}{2} r^2,$$

on aura alors

$$N = x^2 + y^2 \text{ (1)}.$$

Exemples. 1° Soit le nombre

$$N = 1021273028302258913 = \frac{1}{17^2}(2^{68} + 1).$$

On trouve

$$\sqrt{N} = a \doteq 1010580540.$$

Le développement de $\sqrt{N}$ est

$$a\,(4, 4, 2a).$$

Il en résulte que N est de la forme

$$N = (17k + 2)^2 + (8k + 1) = (15k + 2)^2 + (8k + 1)^2,$$

de

$$17k + 2 = a = 1010580540, \qquad \text{on tire} \qquad k = 59445914,$$

$$15k + 2 = 891688712 = x,$$

$$8k + 1 = 475567313 = y, \qquad N = x^2 + y^2.$$

Ces nombres apparaissent d'ailleurs dans le développement de la racine carrée de N, car on trouve successivement

$$\sqrt{N} = a + \frac{1}{x_1}, \qquad x_1 = \frac{\sqrt{N} + a}{y} = 4 + \frac{1}{x_2},$$

$$x_2 = \frac{\sqrt{N} + x}{y} = 4 + \frac{1}{x_3}, \text{ etc.}$$

On trouve encore une solution de $N = x^2 + y^2$ par la considération de $289 = 15^2 + 8^2$ et $(15^2 + 8^2)\,N = 2^{68} + 1$, donnant

$$15x + 8y = 2^{34},$$

$$8x - 15y = 1,$$

qui sont vérifiées par les mêmes valeurs de x et y.

---

(1) Gauss. Œuvres II, p. 89-91.

Enfin, puisqu'on a $(2^{34})^2 \equiv -1$ (Mod. N), on trouve en développant $\frac{2^{34}}{N}$ en fractions continues.

	0	k	7	1	1	1
2^{34}	N	2^{34}	2258944737	1367256025	x	y, etc.
2^{34}			x	y		

donc

$$\frac{2^{34}}{N} = 0, k, 7, 1, 1, 1, \text{etc.}$$

Les réduites de cette fraction sont

		7	1	1	1
0	1	7	8	15	23, etc.
1	k	$7k+1$	$8k+1$	$15k+2$	$23k+3$

Comme $N < (23k+3)^2$, on aura

$$N = (8k+1)^2 + (15k+2)^2 = y^2 + x^2.$$

Ainsi, par trois méthodes qui paraissent indépendantes, on trouve toujours la même décomposition $N = x^2 + y^2$.

Cela peut faire supposer que la décomposition $N = x^2 + y^2$ est unique et N serait alors premier. En réalité, la décomposition $N = x^2 + y^2$ n'est pas unique. On trouve en dehors de la solution envisagée

$$x = 891688712, \qquad y = 475567313,$$

encore la suivante

$$x = 973633432, \qquad y = 270759983.$$

Mais cette deuxième solution ne peut être obtenue que par tâtonnement en résolvant l'équation $N = x^2 + y^2$.

Les deux solutions donnent la décomposition connue (R, p. 92).

2° $N = 165.2^{32} + 1$.

On trouve (Mod. N)

$$497221^2 \equiv -10.2530^2.3^4.89,$$

$$10^2.3.2.11^2.89 \equiv 841829^2,$$

$$840929^2 \equiv -520^2.13^2.11.3,$$

$$5.11.3.2^{32} \equiv -1.$$

Et, en les multipliant membre à membre

$$60152460755^2 + 3.9816567969^2 \equiv 0.$$

Or, ayant la relation $a^2 + 3b^2 \equiv 0$, on trouve en posant $bx = \equiv a$, et en développant $\frac{b}{N}$ en fraction continue

$$\frac{b}{N} = 0,72,5,4,2,1,159,2,7,13,3,1,4,2,26,4.$$

Le dénominateur de l'avant dernière réduite est

$$d = 175508680709.$$

On aura ainsi

$$bd \equiv \pm 1 \qquad \text{ou} \qquad bda \equiv \pm a,$$

d'où

$$x = da \equiv 55843636850$$

et on aura

$$x^2 \equiv -3.$$

Si ensuite on développe $\frac{x}{N}$ en fraction continue, on trouve

$$\frac{x}{N} = 0,12,1,2,4,2,1,1,1,3,1,6,2,1,5, \text{ etc.},$$

dont les réduites se forment facilement.

Le dernier dénominateur inférieur à $\sqrt{N}$ est 805247 et on a

$$N = 805247^2 + 3\,(2^4.17.521)^2.$$

3° $N = 157.2^{32} + 1$. On trouve (Mod. N)

$$29781933^2 \equiv 6901^2.8.2326277,$$

$$2326277.32.37747 \equiv 1866609^2,$$

$$809693^2 \equiv -37747.8.61949,$$

$$61949.8.2077^2 \equiv 1676979^2,$$

d'où, en multipliant ces congruences membre à membre,

$$136834193637^2 + 97086007639^2 \equiv 0.$$

Si on multiplie les deux termes de cette congruence par 49765887059^2 il vient

$$323811094667^2 \equiv -1 \qquad \text{d'où} \qquad N = 648167^2 + 504172^2.$$

10. Soit l'équation $x^2 + Dy^2 = N$ et soit p un module quelconque.

Posons $\qquad \pm x \equiv 0, 1, 2, 3, \ldots, \frac{p-1}{2}$ (Mod. p),

et calculons les valeurs correspondantes de $Dy^2 = N - x^2$

$$Dy^2 \equiv a_0, a_1, a_2, a_3, \ldots. \text{ (Mod. } p).$$

Si, pour une certaine valeur de x, $x = i$, la valeur correspondante de $Dy^2 = a_i$ est un résidu de p, cette valeur $x = i$ est admissible si $\left(\frac{D}{p}\right) = 1$ et inadmissible si $\left(\frac{D}{p}\right) = -1$.

Par contre, si a_i est un non résidu, la valeur correspondante de x, $x = i$ est inadmissible si $\left(\frac{D}{p}\right) = +1$ et admissible si $\left(\frac{D}{p}\right) = -1$.

Cela résulte de ce que D et Dy^2 sont à la fois tous deux résidus ou tous deux non résidus.

Il s'en suit qu'on peut toujours trouver des formes linéaires de x (Mod. p).

Puisque tout nombre a_i est résidu ou non résidu, les nombres $0, 1, 2, 3, \ldots, \frac{p-1}{2}$ se répartissent en deux groupes :

1° Formes linéaires de x dans $x^2 + Dy^2 = N$ quand $\left(\frac{D}{p}\right) = +1$.

2° » » » $\left(\frac{D}{p}\right) = -1$.

Si $a_i \neq 0$, la valeur correspondante de x, $x = i$, fait partie de l'un ou de l'autre groupe. Mais, si $a_i = 0$, la valeur correspondante de x doit figurer dans les deux groupes.

Remarquons qu'on ne trouvera $a_i = 0$ que si $\left(\frac{N}{p}\right) = 1$.

11. Chaque fois que $\left(\frac{N}{p}\right) = +1$, il existe une valeur de x, $x = i$ donnant $a_i = 0$ et cette valeur de x figure aussi bien parmi les valeurs de x dans $x^2 + Dy^2 \equiv N$, quand $\left(\frac{D}{p}\right) = +1$ que dans le cas où $\left(\frac{D}{p}\right) = -1$.

Dans ce cas, la valeur $x \equiv \pm i$ (Mod. p), peut être réduite (Mod. p^2).

En effet, si on considère les valeurs

$$x \equiv kp \pm i \text{ (Mod. } p^2), \qquad \left(k = 0, 1, 2, \ldots, \frac{p-1}{2}\right),$$

et si on calcule les valeurs correspondantes de $Dy^2 = N - x^2 \equiv 0$ (Mod. p), on trouve

$$Dy^2 \equiv lp \text{ (Mod. } p^2), \qquad (l \equiv 0, 1, 2, 3, \ldots, p-1).$$

Toutes ces valeurs de Dy^2 sont $\equiv 0$ (Mod. p), mais seule la valeur $x = kp + i$ donnant $l_h = 0$ peut rendre $y^2 = \frac{N - x^2}{D}$ carré parfait.

Il en résulte que le système complet des solutions de x sera

$\pm x \equiv i_1, i_2, i_3, \ldots$ (Mod. p), donnant y non $\equiv 0$ (Mod. p),

et $\pm x \equiv kp + i$ (Mod. p^2), » $y \equiv 0$ (Mod. p).

Toutefois, l'emploi d'un module p^2 n'est justifié que pour les petites valeurs de p.

12. Ainsi qu'on vient de le voir, on peut toujours trouver les formes linéaires admissibles de x de l'équation $x^2 + Dy^2 = N$ pour un module p quelconque.

Les petites valeurs de p méritent une étude particulière, dont nous allons nous occuper, en commençant par 2 (ou 2^n) — module le plus petit et aussi le plus important.

D'abord l'équation $x^2 + Dy^2 = N$ est évidemment impossible si

$$N \equiv 3 \text{ (Mod. } 4) \quad \text{et} \quad D \equiv 1 \text{ (Mod. } 4), \quad \text{ou} \quad N \equiv 5 \text{ (Mod. } 8),$$

$$\text{et} \quad D \equiv 2 \text{ (Mod. } 4),$$

Dans tous les autres cas, l'équation $x^2 + Dy^2 = N$ est possible (Mod. 2^n), ce qui ne veut cependant pas dire qu'il existe des valeurs de x et y qui la vérifie. La valeur de x peut être avantageusement réduite (Mod. 2^n).

Si d'abord $N \equiv 1$ (Mod. 8) et $D \equiv 1$ (Mod. 4), la valeur de x peut être limitée à 1 cas sur 4, 2 cas sur 64, 2 cas sur 256, etc., de sorte qu'il y a en tout

$$\frac{1}{4} + \frac{1}{2^5} + \frac{1}{2^7} \cdots = \frac{1}{4} + \frac{4}{32\,3} = \frac{1}{4} + \frac{1}{24} = \frac{7}{24}$$

de toutes les valeurs de x à étudier.

Si $D \equiv 2$ (Mod. 4), on aura 2 cas sur 32, 2 sur 128, etc., soit

$$\frac{1}{16} + \frac{1}{64} \cdots = \frac{1}{16} \cdot \frac{4}{3} = \frac{1}{12}$$

de toutes les valeurs de x à étudier.

Si $D \equiv 3$ (Mod. 4), on aura 2 cas sur 32, 2 cas sur 64, 2 sur 256, etc., soit $\frac{1}{24}$ de toutes les valeurs de x à étudier.

Si ensuite $N \equiv 3$ (Mod. 8), on aura à étudier 2 cas sur 8 ou 1 cas sur 4 suivant que $D \equiv 2$ ou 3 (Mod. 4).

Si $N \equiv 5$ (Mod. 8), on aura 2 cas sur 16, aussi bien dans l'équation $x^2 + (4k + 1)\, y^2 = N$ que dans l'équation

$$x^2 + (4k + 3)\, y^2 \equiv N.$$

Si enfin $N \equiv 7$ (Mod. 8), on aura 2 cas sur 32, 2 cas sur 128, etc., soit $\frac{1}{12}$ de tous les cas, si $D \equiv 2$ (Mod. 4) ou bien 1 cas sur 4, si $D \equiv 3$ (Mod. 4).

13. Le module 2^n étant, de loin, le plus important pour l'élimination, nous allons approfondir les résultats obtenus dans le paragraphe précédent.

Soit d'abord $N \equiv 1$ (Mod. 8) et $D \equiv 1$ (Mod. 4).

Soit, pour fixer les idées, $N \equiv 1$ (Mod. 2^a) et $D \equiv 1$ (Mod. 8), a étant supposé suffisamment grand.

Si on pose

$$\pm\, x \equiv 0, 1, 2, 3, 4, 5, 6, 7, 8 \text{ (Mod. 16)},$$

on trouve

$$x^2 \equiv 0, 1, \ 4, \ 9, 16, 25, \ 4, 17, 0 \text{ (Mod. 32)},$$

$$Dy^2 = N - x^2 = 1, 0, 29, 24, 17, \ 8, 29, 16, 1.$$

Il en résulte que si x est pair, on aura $x \equiv 0$ (Mod. 4),

» x impair, » $x \equiv \pm 1$ (Mod. 8).

Les solutions paires ne peuvent plus être réduites, car elles donnent lieu à $Dy^2 \equiv 1$ ou 17 (Mod. 32) — solutions impaires pour y.

Mais les solutions impaires de x donnant lieu à des solutions paires de y peuvent être réduites.

Développons à cet effet, les solutions $x \equiv \pm 1$ (Mod. 8), en solutions (Mod. 64).

$$\pm x \equiv 1, \ 7, \ 9, 15, 17, \ 23, \ 25, 31 \text{ (Mod. 64)},$$

$$x^2 \equiv 1, 49, 81, 97, 33, \ 17, 113, 65 \text{ (Mod. 128)},$$

$$Dy^2 = N - x^2 \equiv 0, 80, 48, 32, 96, 112, \ 16, 64 \text{ (Mod. 128)},$$

$$\frac{1}{16} Dy^2 \equiv 0, \ 5, \ 3, \ 2, \ 6, \ 7, \ 1, \ 4 \text{ (Mod. 8)}.$$

Le seul résidu impair de $\frac{1}{16} Dy^2$ est 1, les solutions 0, 4 sont des solutions paires, qui peuvent être réduites, les autres valeurs sont inadmissibles. On aura donc

$$x \equiv \pm 25 \text{ (Mod. 64)} \quad \text{ou} \quad x \equiv \pm 1 \text{ (Mod. 32)}.$$

Les solutions $x = \pm 1$ (Mod. 32), peuvent être réduites par le module 2^9. A cet effet, développons les solutions $x = \pm 1$ Mod. 32) suivant le module 256, il vient

$$\pm x \equiv 1, \ 31, \ 33, \ 63, \ 65, \ 95, \ 97, 127 \text{ (Mod. 256)},$$

$$x^2 \equiv 1, 449, \ 65, 385, 129, 321, 193, 257 \text{ (Mod. 512)},$$

$$Dy^2 \equiv 0, \ 64, 448, 128, 384, 192, 320, 256 \quad »$$

$$\frac{1}{64} Dy^2 \equiv 0, \ 1, \ 7, \ 2, \ 6, \ 3, \ 5, \ 4 \text{ (Mod. 8)}.$$

La solution $x \equiv \pm 31$ (Mod. 256) est irréductible, les solutions $x \equiv 1, 127$ (Mod. 256), pouvant s'écrire $x \equiv \pm 1$ (Mod. 128), peuvent être réduites par le module 2^{11}, les autres sont inadmissibles.

En continuant, on trouve qu'on aura dans ce cas [$N \equiv 1$ (Mod. 2^a), $D \equiv 1$ (Mod. 8)]

$$x \equiv 0 \text{ (Mod. 4)}, \quad \pm 25 \text{ (Mod. 64)}, \quad \pm 31 \text{ (Mod. } 2^8\text{)},$$
$$\pm 127 \text{ (Mod. } 2^{10}\text{)}, \quad \pm 511 \text{ (Mod. } 2^{12}\text{)}, \quad \pm 2047 \text{ (Mod. } 2^{14}\text{)},$$
$$\pm 8191 \text{ (Mod. } 2^{16}\text{)},$$

etc.,

$$\pm (2^{2k-3} - 1) \text{ Mod. } 2^{2k}), \quad \pm 1 \text{ (Mod. } 2^{2k-1}).$$

Nous avons supposé $N \equiv 1$ (Mod. 2^a) ; mais il en sera de même, si $N \equiv 1$ (Mod. 8) ; la forme des solutions reste la même ; seules, les solutions changent avec la valeur de N.

On peut d'ailleurs donner ces solutions sous une autre forme. Soit donc l'équation

$$x^2 + (8k + 1)\, y^2 = N,$$

N étant supposé de la forme $8l + 1$.

Une des inconnues est paire, l'autre impaire. Celle qui est paire est même divisible par 4. On aura donc

$$x \equiv 0 \text{ (Mod. 4)},$$

ou bien, i désignant un nombre impair

$$y \equiv 4i, \quad x \equiv \sqrt{N - 16} \text{ (Mod. } 2^7\text{)}, \quad \text{ou} \quad x \equiv \pm r_1 \text{ (Mod. } 2^6\text{)},$$
$$y \equiv 8i, \quad x \equiv \sqrt{N - 64} \text{ (Mod. } 2^9\text{)}, \quad \text{ou} \quad x \equiv \pm r_2 \text{ (Mod. } 2^8\text{)},$$
$$y \equiv 16i, \quad x \equiv \sqrt{N - 2^8} \quad \text{ou} \quad x \equiv \pm r_3 \text{ (Mod. } 2^{10}\text{)},$$

etc.

Ces formes peuvent être explicitées dans certains cas, comme nous venons de le voir dans le cas de $N \equiv 1$ (Mod. 2^a).

14. Par le même procédé, on trouve que si $N \equiv 1$ (Mod. 8) et $D \equiv 5$ (Mod. 8), on aura des solutions de la même forme que précédemment.

Développons ces solutions pour le cas de $N \equiv 1$ (Mod. 2^a) et $D \equiv 5$ (Mod. 8).

On trouve que si x est pair, x sera $\equiv 2$ (Mod. 4).

Si x est impair, x sera $\equiv \pm 7$ (Mod. 64) ou ± 1 (Mod. 32).

La dernière solution $x \equiv \pm 1$ (Mod. 32), peut être remplacée par $x \equiv \pm 97$ (Mod. 256), ou ± 1 (Mod. 128).

La solution $x \equiv \pm 1$ (Mod. 128), peut être remplacée par $x \equiv \pm 385$ (Mod. 2^{10}), ou $x \equiv \pm 1$ (Mod. 2^9), etc.

La solution $x \equiv \pm 1$ (Mod. 2^{2k-1})), peut être remplacée par $\pm x \equiv 3.2^{2k-1} + 1$ (Mod. 2^{2k+2}), ou ± 1 (Mod. 2^{2k+1}).

De même, si $N \equiv 1$ (Mod. 8) et $D \equiv 3$ (Mod. 4), conduisent à des solutions analogues, sauf que dans ce cas, x ne peut être pair.

On aura, par exemple, si $N \equiv 1$ (Mod. 2^a) et $D \equiv 3$ (Mod. 8)

$\pm x \equiv 9$ (Mod. 64) ou 95 (Mod. 256) ou 383 (Mod. 1024), ...,

ou $(3.2^{2k-3} - 1)$ (Mod. 2^{2k}) ou 1 (Mod. 2^{2k-1}).

Si $N \equiv 1$ (Mod. 2^a) et $D \equiv 7$ (Mod. 8), on trouvera $\pm x \equiv 23$ (Mod. 64) ou 33 (Mod. 256) ou 129 (Mod. 1024), ...

ou $(2^{2k-3} + 1)$ (Mod. 2^{2k}) ou 1 (Mod. 2^{2k-1}).

15. Considérons ensuite le cas, de D est pair. Nous développerons ce cas quand $N \equiv 1$ (Mod. 2^a), mais on aura des solutions analogues chaque fois que $N \equiv 1$ (Mod. 8).

Si $D \equiv 2$ (Mod. 16), on aura

$$\pm x \equiv 11 \text{ (Mod. 32)}, \quad 15 \text{ (Mod. } 2^7), \quad 63 \text{ (Mod. } 2^9), \quad \text{etc.},$$
$$(2^{2k} - 1) \text{ (Mod. } 2^{2k+3}), \quad 1 \text{ (Mod. } 2^{2k+2}).$$

Si $D \equiv 6$ (Mod. 16), on aura

$$\pm x \equiv 13 \text{ (Mod. 32)}, \quad 47 \text{ (Mod. } 2^7), \quad 191 \text{ (Mod. } 2^9), \quad \text{etc.},$$
$$(3.2^{2k} - 1) \text{ (Mod. } 2^{2k+3}), \quad 1 \text{ (Mod. } 2^{2k+2}).$$

Si $D \equiv 10$ (Mod. 16), on aura

$$\pm x \equiv 5 \text{ (Mod. 32)}, \quad 49 \text{ (Mod. } 2^7), \quad 193 \text{ (Mod. } 2^9), \quad \text{etc.},$$
$$(3.2^{2k} + 1) \text{ (Mod. } 2^{2k+3}), \quad 1 \text{ (Mod. } 2^{2k+2}).$$

Enfin, si $x \equiv 14$ (Mod. 16), on aura

$$\pm x \equiv 3 \text{ (Mod. 32)}, \quad 17 \text{ (Mod. } 2^7), \quad 65 \text{ (Mod. } 2^9), \quad \text{etc.},$$
$$(2^{2k} + 1) \text{ (Mod. } 2^{2k+3}), \quad 1 \text{ (Mod. } 2^{2k+2}).$$

Dans tous ces cas, la valeur de x est limitée à 2 cas sur 32, 2 cas sur 128, 2 cas sur 512, etc., soit à la limite à 1 cas sur 12.

16. Considérons ensuite le cas où $N \equiv 3$ (Mod. 8).

Si $D \equiv 3$ (Mod. 8), on aura $x \equiv 0$ (Mod. 4),

$D \equiv 7$ » » $x \equiv 2$ »

Si $D \equiv 2$ (Mod. 16), » $x \equiv \pm 1$ (Mod. 8),

$D \equiv 10$ » » $x \equiv \pm 3$ »

L'équation $x^2 + Dy^2 \equiv N$ est impossible si $D \equiv 5$ (Mod. 8), [avec $N \equiv 3$ (Mod. 8)].

17. Si $N \equiv 5$ (Mod. 8), on aura dans l'équation $x^2 + Dy^2 = N$ à considérer les cas de $D \equiv 1$ (Mod. 8) et $D \equiv 5$ (Mod. 8).

Voici une table des valeurs de x dans ces cas

$$N \equiv 5,\ 13,\ 21,\ 29 \text{ (Mod. 32)},$$

$$D \equiv 1 \text{ (Mod. 8)}, \quad \pm x \equiv 1,\ 3,\ 7,\ 5 \text{ (Mod. 16)},$$

$$D \equiv 5 \quad » \quad \pm x \equiv 7,\ 5,\ 1,\ 3 \text{ (Mod. 16)}.$$

18. Considérons enfin, le cas de $N \equiv 7$ (Mod. 8).

Si $D \equiv 3$ (Mod. 8), on aura $x \equiv 2$ (Mod. 4),

$D \equiv 7$ » » $x \equiv 0$ »

$D \equiv 6$ (Mod. 16), » $x \equiv \pm 1$ (Mod. 8),

$D \equiv 14$ » » $x \equiv \pm 3$ »

L'équation $x^2 + (8k + 2)\, y^2 = 8l + 7$ est impossible.

Nous remarquerons enfin, que l'équation $x^2 + Dy^2 = N$ se comporte comme l'équation $x^2 - y^2 = N$, pour ce qui est des formes linéaires de x, si $D \equiv 7$ (Mod. 8).

Il en résulte que les formes linéaires de x sont les mêmes dans les équations $x^2 + (8k + 7)\, y^2 = N$ et $x^2 - y^2 = N$.

19. Quel que soit le module impair p envisagé, l'équation $x^2 + Dy^2 = 0$, se comporte comme $x^2 - y^2 = N$, si

$$\left.\begin{array}{lll} \left(\dfrac{D}{p}\right) = +1 & \text{et} & p \equiv 1 \text{ (Mod. 4)}, \\ \left(\dfrac{D}{p}\right) = +1 & \text{et} & p \equiv +3 \text{ (Mod. 4)}. \end{array}\right\} \quad (1)$$

On peut donc, dans ces cas, utiliser les tables que nous avons données p. 156-166.

Ces tables sont encore utilisables, si les conditions (1) ne sont pas satisfaites, mais alors les tables donnent *les valeurs qu'ils ne faut pas prendre* pour x.

On fera, toutefois, exception pour la solution réductible qui doit être prise dans les deux cas.

Exemples. 1° Formes linéaires de x dans $x^2 + 3y^2 \equiv N \equiv 5$ (Mod. 13).

On trouve $\pm x \equiv 1, 2, 3.$

2° Formes linéaires de x dans $x^2 + 7y^2 \equiv 4$ (Mod. 11).

On trouve $\pm x \equiv 4, 8, 9$ ou $\pm x \equiv 2, 3, 4.$

3° Formes linéaires de x dans $x^2 + 7y^2 \equiv 4$ (Mod. 13).

Toutes les valeurs de x sont bonnes, excepté celles données par les tables $\pm 0, 1, 2, 4$. De ces dernières 2 (ou $\sqrt{N}$) est à excepter, donc $\pm x \equiv 2, 3, 5, 6.$

4° Formes linéaires de x dans $x^2 + 2y^2 \equiv 5$ (Mod. 23).

Les valeurs $\pm x \equiv 0, 3, 6, 8, 10, 11,$ sont à rejeter, donc

$$\pm x \equiv 1, 2, 4, 5, 7, 9 \text{ (Mod. 23)}.$$

20. On remarquera que les tables envisagées sont inutilisables, si le module employé est un diviseur de D. Nous allons examiner ce cas.

Soit, d'abord le cas de $D = 3k$ et $p = 3$. On doit avoir $N \equiv 1$ (Mod. 3), D n'est évidemment pas divisible par 9, donc $D \equiv 3$ ou 6 (Mod. 9).

D'autre part, x ne peut pas être $\equiv 0$ (Mod. 3), on aura donc $x^2 \equiv 1$ (Mod. 3).

Les deux termes de l'équation

$$Dy^2 = N - x^2,$$

sont divisibles par 3. Si on supprime ce facteur, on aura $y^2 = \dfrac{N - x^2}{3}$ et ce nombre entier doit être un résidu (Mod. 9).

D'où il résulte la table suivante :

Valeurs de x dans $x^2 + Dy^2 = N$.

D ≡ 3 (Mod. 9).			D ≡ 6 (Mod. 9).	
± x ≡ 4 (Mod. 9)	ou 1 (Mod. 27)	N ≡ 1 (Mod. 27)	± x ≡ 2 (Mod. 9)	ou 1 (Mod. 27)
1	2	4	4	2
2	13	7	1	13
4	8	10	2	8
1	11	13	4	11
2	4	16	1	4
4	10	19	2	10
1	7	22	4	7
2	5	25	1	5

21. Soit encore le cas de $p = 5$, et D ≡ 0 (Mod. 5) ; on doit avoir N ≡ ± 1 (Mod. 5).

On formera, comme précédemment, la table suivante :

Valeurs de x dans $x^2 + Dy^2 = N$.

D ≡ 5 ou 20 (Mod. 25)		D ≡ 10 ou 15 (Mod. 25)
± x ≡ 1, 9, 11 (Mod. 25)	N ≡ 1 (Mod. 25)	± x ≡ 1, 4, 6 (Mod. 25)
2, 3, 7	4	2, 8, 12
1, 6, 9	6	4, 9, 11
2, 3, 8	9	3, 7, 12
4, 6, 9	11	1, 6, 11
3, 8, 12	14	2, 7, 8
4, 6, 11	16	1, 4, 9
7, 8, 12	19	2, 3, 12
1, 4, 11	21	6, 9, 11
2, 7, 12	24	3, 7, 8

On peut former une table analogue pour $p = 7, 11, 13$, mais ces cas étant moins fréquents, la confection d'une table est moins nécessaire. On la formera chaque fois qu'on aura à l'utiliser.

On peut faire, à propos de ces tables, des observations analogues à celles que nous avons faites pour les solutions de x dans $x^2 - y^2 = N$; mais, dans le désir d'abréger, nous ne nous y arrêterons pas.

Bruxelles. — impr. Stevens, rue des fortifications, 9.

CHAPITRE XIV.

Des cycles.

1. Définition. — Étant donnée une suite de congruences de même module

$$a_i\, x_i^2 \equiv b_i\, y_i^2 \,(\text{Mod. N}), \tag{1}$$

($i = 1, 2, 3, \ldots, n$), on dira que ces congruences forment *un cycle*, si le produit de tous les coefficients est un carré parfait, c'est-à-dire, si

$$\prod_{i=1}^{i=n} a_i\, b_i = a_1 a_2 a_3 \ldots a_n \,.\, b_1 b_2 b_3 \ldots b_n = \mathrm{C}^2. \tag{2}$$

Si on fait le produit membre à membre, des congruences (1), on aura

$$a_1 a_2 a_3 \ldots a_n (x_1 x_2 x_3 \ldots x_n)^2 \equiv b_1 b_2 b_3 \ldots b_n (y_1 y_2 y_3 \ldots y_n)^2. \tag{3}$$

Soit d le diviseur commun des

$$a_1 a_2 a_3 \ldots a_n \qquad \text{et} \qquad b_1 b_2 b_3 \ldots b_n\,.$$

On peut poser en vertu de (2)

$$\left.\begin{aligned} a_1 a_2 a_3 \ldots a_n &= d\mathrm{A}^2 \\ b_1 b_2 b_3 \ldots b_n &= d\mathrm{B}^2 \end{aligned}\right| \; \mathrm{C} = d\mathrm{AB}.$$

Posons encore

$$x = x_1 x_2 \ldots x_n, \qquad y = y_1 y_2 \ldots y_n,$$

et (3) devient

$$(\mathrm{A}x)^2 \equiv (\mathrm{B}y)^2. \tag{4}$$

Le cycle sera dit *primitif*, si

$$\mathrm{A}x \equiv \pm\, \mathrm{B}y, \tag{5}$$

et *dérivé*, si la congruence (5) n'a pas lieu.

Si dans (4) on multiplie les deux membres par $d^2\mathrm{A}^2$, il vient

$$(d\mathrm{A}^2 x)^2 \equiv (\mathrm{C}y)^2,$$

ou

$$a_1 a_2 a_2 \ldots a_n x_1 x_2 \ldots x_n \equiv \pm\, \mathrm{C}y, \tag{6}$$

2. Nous aurons à considérer souvent un cycle de congruences d'une forme plus spéciale que celles données par (1). C'est ainsi que le cas particulier $a_i = 1$ ($i = 1, 2, 3, \ldots, n$) se présentera fréquemment.

Nous remarquerons encore que la représentation d'un nombre N par la forme $x^2 + Dy^2$ donne la congruence $x^2 \equiv -Dy^2$ (Mod. N), que nous aurons souvent à utiliser.

D'après les définitions du paragraphe précédent, le cycle formé des n congruences

$$x_i^2 \equiv D_i\, y_i^2 (\text{Mod. N}),$$

sera *primitif*, si dans la congruence résultante

$$x^2 \equiv D^2 y^2,$$

on a $x \equiv \pm Dy$, et *dérivé*, si cette dernière congruence n'a pas lieu. On a posé $D^2 = D_1 D_2 D_3 \ldots D_n$.

3. Exemples. 1° Un cycle peut être constitué par une seule congruence.

Ainsi la congruence

$$(kN \pm x)^2 \equiv x^2 \text{ (Mod. N)},$$

forme un cycle primitif.

La congruence

$$(ka + lb)^2 \equiv (ka - lb)^2 \text{ (Mod. } N = ab),$$

forme un cycle dérivé.

L'équation

$$N = x^2 - y^2,$$

formera un cycle primitif si

$$x = \frac{N+1}{2}, \qquad y = \frac{N-1}{2},$$

et dérivé dans tous les autres cas.

2° Si on a

$$N = x^2 + Dy^2 = z^2 + Dt^2.$$

On formera un cycle de la façon suivante :

On multipliera, membre à membre, les congruences

$$x^2 = -Dy^2 \text{ (Mod. N)},$$

$$z^2 \equiv -Dt^2$$

et on aura

$$(xz)^2 \equiv (\mathrm{D}yt)^2 \text{ (Mod. N)}.$$

Ou bien, on multipliera, membre à membre, les congruences

$$x^2 \equiv -\mathrm{D}y^2 \text{ (Mod. N)},$$

$$\mathrm{D}t^2 \equiv -z^2$$

ce qui donne le cycle

$$(xt)^2 \equiv (yz)^2 \text{ (Mod. N)}.$$

Nous verrons que ce cycle est dérivé, si $\mathrm{D} > 0$.

4. Nous conviendrons de dire que le cycle $\mathrm{A}^2 \equiv \mathrm{B}^2$ (Mod. N), ne diffère pas du cycle $\mathrm{B}^2 \equiv \mathrm{A}^2$ (Mod. N). Sous cette réserve, une seule congruence formant un cycle, donne lieu à un seul cycle. Mais, si le cycle est formé de deux congruences, on peut obtenir deux cycles (exemple 2° du paragraphe précédent). D'une façon générale, n congruences formant un cycle, donnent lieu à 2^{n-1} cycles différents.

Par exemple, les formes

$$\mathrm{N} = x^2 + aby^2 \equiv z^2 + act^2 = u^2 + bcv^2 = w^2 + s^2,$$

donnent lieu aux congruences (Mod. N)

$x^2 \equiv -aby^2$	$x^2 \equiv -aby^2$	$x^2 \equiv -aby^2$	$x^2 \equiv -aby^2$
$z^2 \equiv -act^2$	$z^2 \equiv -act^2$	$z^2 \equiv -act^2$	$z^2 \equiv -act^2$
$u^2 \equiv -bcv^2$	$u^2 \equiv -bcv^2$	$bcv^2 \equiv -u^2$	$bcv^2 \equiv -u^2$
$w^2 \equiv -s^2$	$s^2 \equiv -w^2$	$w^2 \equiv -s^2$	$s^2 \equiv -w^2$

$x^2 \equiv -aby^2$	$x^2 \equiv -aby^3$	$x^2 \equiv -aby^2$	$x^2 \equiv -aby^2$
$act^2 \equiv -z^2$	$act^2 \equiv -z^2$	$act^2 \equiv -z^2$	$act^2 \equiv -z^2$
$u^2 \equiv -bcv^2$	$u^2 \equiv -bcv^2$	$bcv^2 \equiv -u^2$	$bcv^2 \equiv -u^2$
$w^2 \equiv -s^2$	$s^2 \equiv -w^2$	$w^2 \equiv -s^2$	$s^2 \equiv -w^2$

On obtiendra en multipliant ces congruences membre à membre le cycle $\mathrm{A}^2 \equiv \mathrm{B}^2$ (Mod, N)

$\mathrm{A} = xzuw$	$xzus$	$xzvw$	$xzvs$
$\mathrm{B} = abcytvs$	$abcytvw$	$aytus$	$aytuw$

$xtuv$	$xtus$	$cxtvw$	$cxtvs$
$byzvs$	$byzvw$	$yzus$	$yzuw$

5. Théorème — *Si le cycle formé des n congruences*

$$a_i\, x_i^2 \equiv b_i\, y_i^2 \text{ (Mod. } n), \tag{1}$$

($i = 1, 2, 3, \ldots, n$) est primitif, tous les $2^{n-1} - 1$ autres cycles qu'on peut former de ces n congruences en intervertissant les membres de l'une ou plusieurs congruences, le sont aussi. Si ce cycle est dérivé, tous les autres le sont aussi.

On peut énoncer autrement ce théorème en disant que *tous les 2^{n-1} cycles qu'on peut former à l'aide de n congruences, sont de la même nature (primitif ou dérivé).*

Ou encore, on dira que *la nature d'un cycle ne dépend pas de l'ordre dans lequel on écrit les membres de l'une ou plusieurs congruences.*

La démonstration qui suit, nous a été suggérée par M. de la Vallée Poussin.

Si le théorème est vrai pour une seule permutation, il le sera pour un nombre quelconque de permutations, puisque l'on pourra effectuer successivement autant de permutations que l'on voudra.

Cela étant, nous allons démontrer qu'on peut permuter les membres *d'une* congruence sans changer la nature du cycle.

On peut supposer, sans nuire à la généralité, que la congruence dont on permute les membres est la première.

Supposons donc qu'au lieu du cycle formé par (1), on considère les congruences (Mod. N)

$$b_1 y_1^2 \equiv a_1 x_1^2,$$

$$a_2 x_2^2 \equiv b_2 y_2^2,$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

$$a_n\, x_n^2 \equiv b_n\, y_n^2,$$

ou en les multipliant, membre à membre et en se servant des égalités posées, page 195, on aura

$$\frac{d\mathrm{A}^2}{a_1}\, b_1 \frac{x^2}{x_1^2}\, y_1^2 \equiv \frac{d\mathrm{B}^2}{b_1}\, a_1 \frac{y^2}{y_1^2}\, x_1^2.$$

Ou, en tenant compte de la première congruence

$$d\mathrm{A}^2 x^2 \equiv d\mathrm{B}^2 y^2,$$

ce qui prouve que les différents cycles qu'on peut former à l'aide des mêmes congruences, sont de même nature.

6. Ainsi, quand n congruences forment un cycle, il est indifférent de former l'un quelconque des 2^{n-1} cycles. On choisira de préférence celui des cycles qui donne lieu à l'élimination du plus grand nombre de facteurs communs dans les deux membres du cycle.

D'une façon générale, on ne peut pas juger d'avance si les n congruences données constitueront un cycle primitif ou dérivé, sauf dans les cas prévus aux paragraphes 9-12.

7. Si N est premier, tout cycle est primitif.

En effet, un cycle quelconque $A^2 \equiv B^2$ (Mod. N) entraîne $A \pm B \equiv 0$ (Mod. N) puisque N est premier.

La réciproque n'est évidemment pas vraie.

8. Si on obtient un cycle dérivé, le module N est composé.

En effet, puisque $A^2 \equiv B^2$ (Mod. N) et A non $\equiv \pm$ B (Mod. N), le nombre N contient deux facteurs (non nécessairement premiers), dont l'un divise $A + B$, l'autre $A - B$. On trouve ces facteurs en cherchant le plus grand commun diviseur de $A + B$ et de N et celui de $A - B$ et de N.

Exemples. Nombres décomposés par des cycles dérivés.

1° $N = 861.2^{29} + 1$. Si on prend les congruences (Mod. N)

$$672664^2 \equiv -413^2.3.17.1123,$$

$$16.3^7.23.1123 \equiv 680551^2,$$

$$615323^2 \equiv -391^2.8.9.71.107,$$

$$287^2.8.3.17.107 \equiv -677237^2,$$

$$640667^2 \equiv -287^2.8.27.41.71,$$

$$161^2.16.9.59.97 \equiv -663991^2,$$

$$737859^2 \equiv 391^2.8.17.59.67,$$

$$41^2.8.3.17.23.97 \equiv 681011^2,$$

$$679861^2 \equiv 23^2.8.3.41.67,$$

leur produit, membre à membre, se réduit, après suppression des facteurs communs à

$$(672664.2.9.615323.640667.97.737859.679861)^2$$
$$\equiv (59.680551.17.677237.71.663991.391.67.681011)^2,$$

ou à un cycle primitif

$$250503147653^2 \equiv 250503147653^2.$$

Mais les congruences (Mod. N)

$$676145^2 \equiv -56^2.32.27.7.241,$$
$$799^2.16.27.241 \equiv -629111^2,$$
$$683035^2 \equiv 1081^2.8.27.17,$$
$$391^2.8.9.71.107 \equiv -615323^2,$$
$$640667 \equiv -287.8.27.41.71,$$
$$287^2.8.3.17.107 \equiv -677237^2,$$
$$3.7.41.2^{29} \equiv -1,$$

conduisent à un cycle dérivé

$$235717047097^2 \equiv 460924651891^2,$$

et à la décomposition

$$N = 89431.5168743.$$

2° $N = 1 + 409.2^{30}$. On trouve (Mod. N)

$$976169^2 \equiv 713^2.7^2.16.1289,$$
$$517^2.8.7.1289 \equiv -647971^2,$$
$$661761^2 \equiv -29^2.2^9.7.409,$$
$$709823 \equiv 329^2.2^7.7.23.29,$$
$$287.2^7.7.23.29 \equiv -624447^2,$$
$$409.2^{30} \equiv -1.$$

Le produit de ces congruences est, les facteurs communs étant écartés

$$(1024.451.976169.661761.709823)^2 \equiv (713.203.647971.624447)^2$$

d'où

$$50511214193^2 \equiv 132469785291^2,$$

et

$$N = 14621.30036277.$$

3° $N = 1 + 809.2^{29}$. On trouve (Mod. N)

$$825153^2 \equiv 4930^2.32.317,$$

$$64.11.29.317 \equiv 659041,$$

$$606053 \equiv 8.5^4.11.29^3,$$

d'où

$$N = 14251.30477059.$$

4° $N = 1 + 531.2^{29}$. On trouve (Mod. N)

$$159135^2 \equiv -437^2.64.53.401,$$

$$301^2.8.3.43.401 \equiv -497579^2,$$

$$817^2.32.3.43.53 \equiv 656593^2,$$

d'où

$$(159135.301.43^2.6)^2 \equiv 23.497579.656593,$$

d'où

$$N = 121789.2340759.$$

5° $N = 1 + 721.2^{28}$. On trouve

$$439935^2 \equiv 2^8.7^2.67,$$

$$1609^2.7^2.67 \equiv 449490^2,$$

d'où

$$N \equiv 20717.9342191.$$

6° $N = 1 + 459.2^{30} = 492847497217$.

On trouve

$$N = 993921^2 - 799^2.2^8.13.233 = 681701^2 + 221^2.8.3.103.233$$
$$= 702001^2 + 32.27.11.13.103 = 702539^2 - 59^2.8.27.13.73$$
$$= 59873^2 + 901^2.64.3.43.73 = 388655^2 + 611^2.17^2.32\text{-}9.11.$$

En multipliant, membre à membre, les congruences (Mod. N)

$$993921^2 \equiv 799^2.2^8.13.233,$$

$$221^2.8.3.103.233 \equiv -681701^2,$$

$$702001^2 \equiv -32.27.11.13.103,$$

$$59^2.8.27.13.73 \equiv 702539^2.$$

$$59873^2 \equiv -901^2.64.3.43.73,$$

$$611^2.17^2.32.9.11 \equiv -388655,$$

on trouve, après avoir supprimé les facteurs communs

$$(993921.13.702001.59.59873.39)^2 \equiv (16.681701.43.702539.53.388655)^2,$$

ou

$$355615034699^2 \equiv 457510529096^2,$$

ou enfin

$$101895494397.320278066578 \equiv 0 \text{ (Mod. N)}.$$

Le plus grand commun diviseur du premier facteur et de N est 13877, celui du second facteur et de N est 35515421 et

$$N = 13877.35515421.$$

$N = 453.2^{30} + 1$. On trouve (Mod. N)

$$697295^2 \equiv -11^2.35.3^4.19.31,$$

$$32.3^7.49.31 \equiv 697457^2,$$

$$697721^2 \equiv 23^2.127^2.16.3,$$

$$209^2.16.97^2 \equiv -692697^2,$$

d'où, en multipliant ces congruences, membre à membre, $A^2 \equiv B^2$.

En cherchant le plus grand commun diviseur de $A + B$ et N et de $A - B$ et N, on trouve les facteurs

$$N = 135433.3591481.$$

7° $N = 1 + 903.2^{29}$. On trouve (Mod. N)

$$1321991^2 \equiv 53^2.29^2.3.7.43.37,$$

$$53^2.16.3.37.593 \equiv 698393^2,$$

$$635857^2 \equiv -29^2.41^2.32.3.593,$$

$$2^{29}.3.7.43 \equiv -1,$$

dont le produit, membre à membre, donne

$$(1321991,635857.4096)^2 \equiv (29^2.41.698393)^2,$$

ou

$$76192371778^2 \equiv 24081289033^2,$$

ou

$$100273660811.5211082745 \equiv 0,$$

d'où

$$N = 25537.18984001.$$

8° $N = 1 + 875.2^{29}$. On trouve (Mod. N)

$$957299^2 \equiv 1430^2.2.13.31.271,$$

$$271.131.18.110^2 \equiv -682251^2,$$

$$32.5.19.13.31 \equiv -685391^2,$$

$$725999^2 \equiv 2^5.5^9.7\ 131,$$

$$770^2.4.5.11.19 \equiv 704999^2,$$

$$685381^2 \equiv -13^2.8.5.47^2,$$

$$2^{29}.5^3.7 \equiv -1,$$

d'où, en multipliant et en supprimant les facteurs communs

$$(957299.725999.685381\ 121.19.32768)^2 \equiv (97913.845.47.682251.704999)^2,$$

d'où

$$N = 291089.1613809.$$

9° $N = 1 + 403^2 .2^{30}$. On trouve (Mod. N)

$$657995^2 \equiv 59^2.8.8599,$$

$$403^2.8.8599 \equiv 666251^2,$$

d'où

$$(657995.443)^2 \equiv (59.666251)^2,$$

d'où

$$N = 8527.50746799.$$

10° $N = 449.2^{27} + 1$. On trouve

$$262145^2 \equiv 2^{19}.127^2 \text{ (Mod. N)},$$

$$2^7.77^2.53^2 \equiv 249791^2,$$

d'où

$$N = 10711.5626343.$$

11° $N = 223.2^{28} + 1$

$$262145^2 \equiv 2^{19}.61.277 \text{ (Mod. N)},$$

$$8.19^2.61.277 \equiv 244765^2,$$

d'où

$$N = 146023.470943.$$

12° $N = 1 + 369.2^{30}$. On trouve (Mod. N)

$$629351^2 \equiv -16.23^2.9.41^2,$$

$$640045^2 \equiv 8.81.13^2.122789,$$

$$533^2.8.122789 \equiv -342267^2,$$

d'où

$$(640045.629351)^2 \equiv (342267.23.4.27)^2,$$

ou

$$7452418966.575203651 \equiv 0,$$

ou

$$N = 7577.52291241.$$

13° $N = 1 + 633.2^{29}$. On trouve (Mod. N)

$$583821^2 \equiv 29^2\ 8.13.281.41,$$

$$114571.16.9.13.281 \equiv -528745^2,$$

$$616965^2 \equiv 211^2.8.114571,$$

$$1189^2.7.131.211 \equiv -165003^2,$$

$$549340^2 \equiv 1537^2.3.41.131,$$

$$211.3.2^{29} \equiv -1,$$

d'où

$$(583821.616965.549340.2^{15})^2 \equiv (528745.55001.1537)^2,$$

et

$$N = 100699.3374803.$$

14° $N = 1 + 289.2^{30}$. On trouve (Mod. N)

$$573953^2 \equiv 2^{10}.17^2.64577,$$

$$1927^2.64577 \equiv -265548^2,$$

$$17^2.2^{30} \equiv -1.$$

d'où

$$(573953.1927.2^{10})^2 \equiv 265548^2,$$

et

$$N = 93253.3327629.$$

15° $N = 765.2^{28} + 1$. On trouve

$$717469^2 \equiv 953^2.8.5.3.17.167,$$

$$31^2.5^3.32.3.167 \equiv 455279^2,$$

$$16.25.3^{12}.17 \equiv 457129^2,$$

d'où

$$(717469.31.200.729)^2 \equiv (457129.455279.953)^2,$$

et

$$N = 52543.3908287.$$

16° $N = 165.2^{32} + 1$. On trouve (Mod. N)

$$567689^2 \equiv -5.16.3.11.17^3.31.31^2,$$

$$3.17.31.2^{12}.5^2 \equiv -841729^2,$$

$$3.2^8.17^2.521^2 \equiv -805247^2,$$

$$5.11.3.2^{32} \equiv -1,$$

d'où, en multipliant ces congruences membre à membre

$$374719014330^2 \equiv 460373802564,$$

ou

$$42827394117.417546408447 \equiv 0,$$

ou

$$N = 33909259.20899.$$

17° $N \equiv 833.2^{29} + 1$. On trouve

$$605739^2 \equiv -497^2.8.179.227,$$

$$8.11.67.179 \equiv 668741^2,$$

$$11^2.64.7.11.227 \equiv -668639^2,$$

$$230399^2 \equiv -511^2.2^{11}.11.67,$$

$$881313^2 \equiv 427^2.64.11.17.151,$$

$$901^2.8.7.61.151 \equiv 168741^2,$$

$$997396^2 \equiv 4081^2.7^2.11.61,$$

$$371^2.32.11.61^2 \equiv -516655^2,$$

$$1 \equiv -17.7^2.29^2,$$

d'où la décomposition

$$N = 230779.1937843.$$

18° $N \equiv 1 + 627.2^{24}$. On trouve (Mod. N)

$$101333^2 \equiv -187^2.3.8.13.23,$$

$$32.187^2.27.13.23 \equiv -38543^2,$$

d'où

$$(101333.6)^2 \equiv 38543,$$

et

$$N = 92363.113891.$$

19° $N = 1 + 765.2^{24}$. On trouve (Mod. N)

$$(113151.384)^2 \equiv 19^2,$$

d'où

$$N = 9157.1401613.$$

9. Théorème. — Deux formes du même déterminant négatif constituent un cycle dérivé.

Soit $$N = ax^2 + by^2 = az^2 + bu^2,$$

ce qui donne lieu aux cycles

$$(axz)^2 \equiv (byu)^2, \qquad \text{ou} \qquad (xu)^2 \equiv (yz)^2.$$

Si $ab > 1$, on aura $xu \pm yz$ non $\equiv 0$ (Mod. N), car

$$N^2 = (ax^2 + by^2)(az^2 + bu^2) = (axz \pm byu)^2 + ab\,(xu \mp yz)^2,$$

et $xu \pm yz \equiv 0$ (Mod. N), entraînerait $xu \pm yz = 0$, ou

$$\frac{x^2}{z^2} = \frac{y^2}{u^2} = \frac{ax^2 + by^2}{az^2 + bu^2} = 1, \qquad \text{d'où} \qquad x = z, \qquad \text{et} \qquad y = u.$$

Si $ab = 1$ (donc $a = b = 1$), on peut prendre $xu \pm yz = N$, mais alors $axz \pm byu = 0$, d'où encore (puisque $a = b = 1$), $x = u$, $y = z$.

10. Théorème. — Les deux formes à déterminant positif

$$N = x^2 - Dy^2 = z^2 - Du^2,$$

constituent un cycle dérivé, si x, y, z et u satisfont aux inégalités

$$\sqrt{N} < x \text{ ou } z < \sqrt{\frac{\alpha + 1}{2} N}, \quad 0 < y \quad \text{ou} \quad u < \sqrt{\frac{\alpha - 1}{2D} N},$$

α et β étant les plus petits nombres vérifiant l'équation

$$\alpha^2 - D\beta^2 = +1 \ (\alpha > 1, \ \beta \neq 0).$$

En d'autres termes, les deux formes à déterminant positif

$$N = a^2 - Db^2 = c^2 - Dd^2,$$

constituent un cycle dérivé, si les solutions (ab), (cd) de l'équation $x^2 - Dy^2 = N$ sont primitives (T. II, p. 176-179).

On aura, en effet (Mod. N)

$$a^2 \equiv Db^2,$$

$$Dd^2 \equiv c^2,$$

ce qui donne

$$a^2d^2 \equiv b^2c^2,$$

ou

$$(ad + bc)(ad - bc) > 0,$$

or $ad \pm bc$ est différent de 0 (Mod. N), car

$$(a^2 - Db^2)(c^2 - Dd^2) = N^2,$$

ou

$$(ac \pm Dbd)^2 - D(ad \pm bc)^2 = N^2, \qquad (6)$$

et $ad \pm bc \equiv 0$ (Mod. N), entraînerait $ac \pm Dbd \equiv 0$ et (6) deviendrait

$$\left(\frac{ac \pm Dbd}{N}\right)^2 - D\left(\frac{ad \pm bc}{N}\right)^2 = 1,$$

on aura donc, par cette relation, une solution de l'équation $x^2 - Dy^2 = 1$, plus petite que la solution $x = \alpha$, $y = \beta$, car $\frac{ac \pm Dbd}{N} < \alpha$, puisque α est le maximum de l'expression $\frac{ac \pm Dbd}{N}$ quand on fait

$$a = c = \sqrt{\frac{\alpha + 1}{2} N}, \qquad b = d = \sqrt{\frac{\alpha - 1}{2D} N}.$$

Puisque α est supposé être la plus petite solution (supérieure à l'unité) de l'équation $x^2 - Dy^2 = 1$, il faut que $ad \pm bc$, soit différent de 0 (Mod. N), ce qui prouve que le cycle (a, b), (c, d) est dérivé.

11. Théorème.— Une solution primitive de l'équation $x^2 - Dy^2 = N$ et sa dérivée (T. II, p. 176-170) forment un cycle primitif.

Soit

$$a^2 - Db^2 = \pm N,$$

et

$$x^2 - Dy^2 = \pm N, \qquad (5)$$

avec

$$x = \pm (a\alpha - Db\beta), \qquad y = \pm (a\beta - b\alpha).$$

On tire de (5)

$$a^2y^2 \equiv b^2x^2 \text{ (Mod. N)},$$

ou

$$ay \pm bx \equiv 0,$$

or

$$ay \pm bx = \pm a(a\beta - b\alpha) \pm b(a\alpha - Db\beta) \equiv 0.$$

12. Toute solution (ab) peut être remplacée par sa dérivée (AB), et cette nouvelle solution (AB) formera avec une autre solution (cd), un cycle de même nature (primitif ou dérivé) que la solution ab.

Soit (AB) une solution dérivée de (ab)

$$A = \pm (a\alpha - Db\beta), \qquad B = \pm (a\beta - b\alpha).$$

L'expression $Ad \pm Bc$ sera 0 ou différente de 0, en même temps que $ad \pm bc$, car

$$Ad \pm Bc = \pm (a\alpha - Db\beta)\, d \pm (a\beta - b\alpha)\, c$$

$$= (ad \pm bc)\, \alpha \pm (ac \pm Db\beta)\, \beta. \qquad (7)$$

Or

$$(a^2 - Db^2)(c^2 - Dd^2) = (ac \pm Dbd)^2 - D\,(ad \pm bc)^2 = N^2,$$

montre $ad \pm bc$ et $ac \pm Dbd$, sont simultanément nuls ou différents de 0 (Mod. N). Il en sera donc de même de $Ad \pm Bc$ et $ad \pm bc$.

13. Si le nombre donné présente peu de résidus parmi les petits nombres 3, 5, 7, 11, ..., on considérera un multiple convenablement choisi du nombre donné λN, de telle façon que λN soit résidu pour un grand nombre de petits facteurs.

Il est entendu qu'on cherchera à former un cycle dérivé, car si on se propose de factoriser N par la mise sous la forme $x^2 - y^2$, on n'aura aucun avantage à rendre λN résidu des petits facteurs.

Mais, si un cycle dérivé peut être formé, il est plus facile de l'obtenir pour λN que pour λ.

Exemple. Le nombre $N = 1 + 619.2^{26}$ est non résidu pour tous les modules inférieurs à 50 excepté 19, 43 et 47.

Mais, si on considère le nombre $17N = N'$. On trouve (Mod. N)

$$843001^2 \equiv 77^2.32.3.11.23.31,$$

$$8.5.3^{10}.31.41^2 \equiv 910643^2,$$

$$8.5^2.3^6,23.887 \equiv 842117^2,$$

$$840343^2 \equiv -2^8.5.9.887,$$

$$2^7.3^3.11.31 \equiv 17.49433^2,$$

$$17.50201^2 \equiv 2^7.5^5.3.7.31,$$

$$372311^2 \equiv -1321^2.2^7.2.7.11^2,$$

dont le produit se réduit à

$$351729613770^2 \equiv 184582324651^2,$$

(Mod. N' et *à fortiori* Mod. N), d'où

$$N = 5569163.7459.$$

CHAPITRE XV.

De l'équation $x^2 - y^2 = N$.

II. Limites de x et y et applications.

1. On sait que l'équation indéterminée $x^2 + Dy^2 = N$, si elle est possible, admet un nombre limité de solutions. Par contre, l'équation $x^2 - Dy^2 = N$ en admet, lorsqu'elle est possible, une infinité, à la condition cependant que D ne soit pas un carré parfait (T. II, p. 73).

Si D est un carré parfait, le développement de $\sqrt{D}$ en fractions continues n'existe plus ; il n'est donc plus possible de déduire d'une première solution de $x^2 - Dy^2 = N$, autant d'autres solutions que l'on voudra, au moyen de celles de l'équation de Pell $x^2 - Dy^2 = 1$.

Nous dirons donc que l'équation $x^2 - Dy^2 = N$ admet, lorsqu'elle est possible, une infinité de solutions, sauf dans le cas où D est un carré parfait. Dans ce dernier cas, l'équation est toujours possible (au moins en nombres rationnels) et admet un nombre fini de solutions.

Nous dirons pour abréger le langage, que le couple des valeurs entières de x et y définit un *point entier*. On énoncera donc ce qui vient d'être dit de la façon suivante. *Le nombre de points entiers sur une ellipse* $x^2 + Dy^2 = N$ *est fini. Le nombre de points entiers d'une hyperbole* $x^2 - Dy^2 = N$ *est infini*, sauf quand cette hyperbole est équilatère $x^2 - y^2 = N$ [1].

2. Dans ce qui suit, nous nous occuperons précisément de l'hyperbole équilatère $x^2 - y^2 = N$.

Il peut arriver que cette équation n'ait pas de solutions entières, par exemple, si $N \equiv 2$ (Mod. 4). Mais dans les conditions ou

---

[1] L'équation $x^2 - Dy^2 = N$, ne diffère pas de $x^2 - y^2 = N$, si D est un carré parfait.

nous avons à l'utiliser, c'est-à-dire, quand il s'agit de factoriser à l'aide de cette équation un nombre donné, N est impair et l'équation est possible. On connaît même une solution

$$x = \frac{N+1}{2}, \qquad y = \frac{N-1}{2},$$

qui correspond au *dernier point entier*, car si on augmente la valeur de x, la différence $x - y$ diminue et on aura $x - y < 1$, donc y ne sera plus jamais entier, si x l'est et inversement.

Si donc, on trouve d'autres solutions que

$$x = \frac{N+1}{2}, \qquad y = \frac{N-1}{2},$$

on aura une décomposition de N, mais la solution citée fournit une décomposition connue $x + y = N$, $x - y = 1$.

3. Soit a et b ($a < b < \sqrt{N}$) deux limites entre lesquelles on se propose de situer le plus petit facteur. On aura donc

$$a < x - y < b \leqslant \sqrt{N},$$

$$\frac{N}{a} > x + y > \frac{N}{b} \geqslant \sqrt{N}.$$

Comme le produit des deux facteurs est constant, leur somme (ainsi que leur demi-somme x) sera minimum quand les deux facteurs seront égaux et cette somme augmente quand les facteurs s'écartent l'un de l'autre. On aura ainsi

$$\sqrt{N} \leqslant \frac{1}{2}\left(b + \frac{N}{b}\right) < x < \frac{1}{2}\left(a + \frac{N}{a}\right).$$

Puisque y varie de la même façon que x, c'est-à-dire, y augmente quand x augmente et inversement, on aura

$$\frac{1}{2}\left(\frac{N}{b} - b\right) < y < \frac{1}{2}\left(\frac{N}{a} - a\right).$$

Pour trouver un facteur compris entre a et b, il faut étudier toutes les valeurs de x et y entre les limites envisagées.

Toutefois, il n'est pas nécessaire d'étudier x et y ; il suffit d'étudier l'une de ces quantités, car si on trouve x, on calculera y par des opérations directes.

Il est préférable de prendre comme inconnue, la quantité dont les limites sont moins éloignées l'une de l'autre.

Calculons donc la différence des limites.

On trouve pour x

$$\frac{1}{2}\left(a+\frac{N}{a}\right)-\frac{1}{2}\left(b+\frac{N}{b}\right)=\frac{(N-ab)(b-a)}{2ab},$$

pour y

$$\frac{1}{2}\left(\frac{N}{a}-a\right)-\frac{1}{2}\left(\frac{N}{b}-b\right)=\frac{(N+ab)(b-a)}{2ab}.$$

Il est préférable de prendre comme inconnue x plutôt que y. Pour trouver un facteur compris entre a et b, on aura à étudier les $\frac{(N-ab)(b-a)}{2ab}=M$ nombres compris entre $\frac{1}{2}\left(b+\frac{N}{b}\right)$ et $\frac{1}{2}\left(a+\frac{N}{a}\right)$.

La forme de M montre que M n'est jamais négatif dans les hypothèses que nous envisageons $(a < b \leqslant \sqrt{N})$.

De plus, M diminue quand a augmente. On aura donc intérêt à prendre a aussi grand que possible.

Ainsi, il est infiniment plus facile de trouver, par ce procédé, des grands facteurs que des petits. Aussi, convient-il de s'assurer que le nombre donné n'a pas des petits facteurs.

Ainsi, si $N > 10^{16}$, il est plus facile d'étudier tous les facteurs compris entre 10^7 et 10^8, que ceux compris entre 10^4 et 10^5. En d'autres termes, bien que le premier intervalle soit mille fois plus grand que le second, son étude est mille fois plus facile.

4. Afin d'augmenter le plus petit facteur et de l'approcher de l'autre, il convient parfois d'introduire un facteur complémentaire et d'envisager la factorisation de λN.

Soit comme précédemment

$$a < x - y < b \leqslant \sqrt{N}.$$

On trouvera ce facteur par l'étude de $\frac{(N-ab)(b-a)}{2ab}$ nombres compris entre les limites de x

$$\frac{1}{2}\left(b+\frac{N}{b}\right) < x < \frac{1}{2}\left(a+\frac{N}{a}\right).$$

Si on considère le nombre $\lambda N = \lambda(x - y), (x + y)$, on aurà

$$a\lambda < \lambda(x - y) < b\lambda \leqslant \sqrt{\lambda N},$$

donnant

$$\frac{1}{2}\left(\lambda b + \frac{N}{b}\right) < x < \frac{1}{2}\left(\lambda a + \frac{N}{a}\right).$$

On aura ainsi

$$M' = \frac{1}{2}\left(\lambda a + \frac{N}{a}\right) - \frac{1}{2}\left(\lambda b + \frac{N}{b}\right) = \frac{(N - \lambda ab)(b - a)}{2ab},$$

valeurs de x à examiner, au lieu

$$M = \frac{(N - ab)(b - a)}{2ab},$$

valeurs de x comme dans le cas général.

On réalisera ainsi une économie de

$$\frac{(N - ab)(b - a)}{2ab} - \frac{(N - \lambda ab)(b - a)}{2ab} = \frac{1}{2}(b - a)(\lambda - 1)$$

essais.

On voit qu'on a intérêt à prendre λ aussi grand que possible, afin d'accentuer l'économie réalisée, mais la condition

$$a\lambda < \lambda(x - y) < b\lambda < \sqrt{\lambda N},$$

qui donne

$$\lambda b^2 < N.$$

montre que λ ne peut dépasser une certaine limite.

De plus, dans le choix de λ, on tâchera de tenir compte des désiderata qu'on s'imposera et dont nous allons énumérer quelques-uns.

1° On ne perdra pas les connaissances acquises sur les facteurs de N.

Ainsi, si on connaît certains résidus R_1, R_2, R_3 ... de N, λ sera choisi tel que ces mêmes nombres en soient résidus. Ils seront donc aussi résidus de λN.

2° Si N (ou son multiple) est de la forme $a^k \pm b^k$, tous les facteurs de N sont de la forme $k\rho + 1$ et λ sera choisi aussi de la forme $k\rho + 1$.

3° Dans le choix de λ, on tiendra compte de ce que λN doit être soumis à une décomposition. Par conséquent, on choisira λ de façon à ce que λN devienne résidu pour un grand nombre de petits facteurs, si on se propose de rechercher les résidus de λN et si N est lui-même résidu de ces facteurs.

Par contre, il est préférable que λN soit non résidu pour les petits facteurs, si on se propose d'attaquer directement l'équation

$$x^2 - y^2 = \lambda N$$

et si N est non résidu pour ces facteurs.

4° En aucun cas, on ne prendra pour λ des nombres divisibles par des petits facteurs 3, 5, 7, 11, ..., devant servir comme modules pour limiter la valeur de x.

5. Applications.— Le procédé que nous allons exposer, trouve son origine dans les deux méthodes que nous avons envisagées.

Soit N un nombre pour lequel on possède plusieurs représentations quadratiques

$$N = x^2 \pm Dy^2.$$

Supposons qu'on ne soit pas parvenu à former un cycle dérivé et que cependant le nombre N soit composé.

Alors, on formera plusieurs résidus r_1, r_2, r_2, ... du nombre N.

Les non résidus n (qui sont toutefois résidus jacobiens) formeront par leur combinaison des résidus

$$n_1 n_2, \qquad n_1 n_3, \qquad n_2 n_3, \qquad \ldots.$$

A l'aide de ces résidus, on achèvera la décomposition par la forme $x^2 - y^2$, en utilisant les résidus à un double point de vue :

1° Pour trouver un facteur éventuel inférieur à une limite donnée ($\sqrt[3]{N}$, 10^4, ou 10^6 ou 10^7 suivant le cas).

2° Pour faciliter l'élimination des valeurs de x pouvant satisfaire à $x^2 - y^2 = N$.

Exemple 1. Soit le nombre $N = 535.2^{30} + 1$.

On trouve que les nombres -1, 2, 7, 13, 41, 47, 83 sont résidus de N.

Il en est de même de 5.29 (T. II, p. 127).

A l'aide de ces résidus, on constate sans peine que N n'a pas de facteurs inférieurs à 10000.

Posons

$$N = a^2 - b^2, \qquad \sqrt{N} < a < \frac{1}{2}\left(10^4 + \frac{N}{10^4}\right).$$

On peut supposer que 5 n'est pas résidu de N, puisqu'on ne parvient pas à isoler le résidu ± 5 [1], les deux facteurs sont donc $\equiv 3$ et 7 (Mod. 10), dès lors $a \equiv 0$ (Mod. 5).

Comme, d'autre part, $a \equiv 1$ (Mod. 32) $\equiv 0$ (Mod. 3), on posera

$$a = 480x + 758145, \qquad 0 < x < 58269.$$

Posons

$$x \equiv 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7 \text{ (Mod. 8)},$$

$$a \equiv 480 + 758145 \equiv 129,\ 97,\ 65,\ 33,\ 1,\ 225,\ 193,\ 161.$$

Les seules solutions admissibles sont $x \equiv 0, 3, 4$ (Mod. 8).

D'autre part $N \equiv 4$ (Mod. 7), ce qui aurait donné $a \equiv \pm 1, 2$ (Mod. 7), mais ± 7 étant résidu, on aura

$$a + b \equiv 1, 9, 11 \text{ (Mod. 14)}, \qquad N \equiv 4 \text{ (Mod. 7)} \equiv 11 \text{ (Mod. 14)},$$

$$a - b \equiv 11, 9, 1$$

$$a \equiv 6, 2 \quad \text{(Mod. 7)}.$$

Or

$$x \equiv 0, 1, 2, 3, 4, 5, 6 \text{ (Mod. 7)},$$

donne

$$a \equiv 4x + 3 \equiv 3, 0, 4, 1, 5, 2, 6,$$

d'où

$$a \equiv 5, 6 \text{ (Mod. 7)}.$$

De même ± 13 étant résidu, on aura

$$a + b \equiv 1,\ 3,\ 9, 17, 23, 25 \text{ (Mod. 26)}, \qquad N \equiv 25 \text{ (Mod. 26)},$$

$$a - b \equiv 25, 17, 23,\ 3,\ 9,\ 1,$$

$$a \equiv 0, 10,\ 3,$$

---

[1] On peut s'en assurer en cherchant la solution de $N = x^2 + 5y^2$. On ne trouvera aucune solution de cette équation. Si d'ailleurs, 5 était un résidu, on serait quitte en essayant à la suite de l'hypothèse $a \equiv 0$ (Mod. 5), l'autre hypothèse $x \equiv \pm 4$ (Mod. 25).

$$x \equiv 0,\ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 \text{ (Mod. 13)},$$

$$a \equiv 12x + 11 \equiv 11,\ 10, 9, 8, 7, 6, 5, 4, 3, 2,\ 1,\ 0, 12,$$

d'où

$$x \equiv 1, 8, 11 \text{ (Mod. 13)}.$$

Ainsi

$$x \equiv 1, 2, 6 \text{ (Mod. 8)} \equiv 5, 6 \text{ (Mod. 7)} \equiv 1, 8, 11 \text{ (Mod. 13)},$$

On trouve

$$x = 7720, \qquad \text{donnant} \qquad a = 4463745,$$

$$b = 4398928,$$

$$a + b = 8862673, \qquad a = b = 64817,$$

$$N = 64817.8862673.$$

Si la décomposition n'avait pas réussi avec $a \equiv 0$ (Mod. 5), on aurait essayé maintenant l'autre hypothèse $a \equiv \pm 4$ (Mod. 25), ce qui présume que 5 est résidu de N, qui aurait été isolé en continuant la recherche des formes $x^2 \pm Dy^2 = N$.

Exemple 2. Soit le nombre $N = 219.2^{29} + 1$.

On a vu (T. II, p. 127), que les nombres $+2$, -3, $+5$, -7, sont résidus de N.

D'autre part N est composé, car la congruence $2^{N-1} \equiv 1$ (Mod. N), n'est pas vérifiée.

On vérifie à l'aide des résidus connus, que N n'a pas des facteurs inférieurs à 10^4.

Posons

$$N = x^2 - y^2, \qquad \text{on aura} \qquad \sqrt{N} < x < \frac{1}{2}\left(10^4 + \frac{N}{10^4}\right),$$

ou

$$342891 < x < 5883736.$$

Il y a lieu de supposer que (-1) n'est pas résidu, car autrement les résidus se séparent facilement. Autrement dit, les deux facteurs (il n'y en a pas plus, puisqu'il n'y a pas de facteurs inférieurs à $10000 > \sqrt[3]{N}$) seront de la forme $8k - 1$.

Ainsi

$$a \equiv -1 \text{ (Mod. 32)} \equiv \pm 4 \text{ (Mod. 9)} \equiv \pm 2 \text{ (Mod. 25) ou } 0 \text{ (Mod. 5)}.$$

Mais -3 étant résidu, on aura $\quad a \equiv +4$ (Mod. 9).

$+5$ $\qquad a \equiv 0$ (Mod. 5).

Ainsi

$$a \equiv -1 \,(\text{Mod.}\,32) \equiv +4 \,(\text{Mod.}\,9) \equiv 0 \,(\text{Mod.}\,5) \quad \text{ou} \quad a \equiv 895 \,(\text{Mod.}\,1440).$$

Posons

$$a = 1440x + 343615, \qquad 0 \leqslant x \leqslant 3837.$$

On trouve

$$\begin{aligned} x \equiv\ & 1, 2 \text{ ou } 6 && (\text{Mod. } 8), \\ & 1, 4, 5, 7 && (\text{Mod. } 9), \\ & 1, 4 && (\text{Mod. } 7), \\ & 0, 5, 6, 8, 10 && (\text{Mod. } 11), \\ & 0, 1, 7, 8, 10, 11 && (\text{Mod. } 13), \\ & 2, 4, 5, 6, 12, 13, 14, 16 && (\text{Mod. } 17), \\ & 0, 1, 6, 7, 9, 10, 12, 13, 18 && (\text{Mod. } 19), \end{aligned}$$

$$x = 50 \qquad \text{donne} \qquad a = 415615, \qquad b = 234864,$$

$$N = 180751.650489.$$

Exemple 3. $N = 927.2^{30} + 1$.

On trouve les résidus suivants -1, 2, 5, 7, 11, 17, 3.13, mais on n'arrive pas à isoler les résidus 3 et 13.

Donc deux cas peuvent se présenter :

1° Le nombre N est premier. Alors les résidus 3 et 13 s'isoleraient, si on continue à chercher d'autres formes $x^2 \pm Dy^2$ plus convenables. Il y a une forte présomption qu'il en soit ainsi, puisque presque tous les résidus de Jacobi sont aussi résidus de Legendre.

Cette hypothèse n'est pas vérifiée, puisque la congruence $2^{N-1} \equiv 1$, n'ayant pas lieu, le nombre N est *composé*.

2° Il est alors à *présumer* que 3 et 13 sont non résidus de N et les autres nombres sont résidus.

Le nombre N se compose alors de deux facteurs (on vérifiera facilement à l'aide de ces résidus que le nombre N n'a pas plus de deux facteurs). Posons

$$N = x^2 - y^2.$$

On trouve

$$x \equiv 33 \,(\text{Mod. } 256) \quad \text{ou} \quad 129 \,(\text{Mod. } 1024) \quad \text{ou} \quad 153 \,(\text{Mod. } 8^{12}), \text{ etc.},$$

$$\equiv 8 \,(\text{Mod. } 9) \equiv 0 \,(\text{Mod. } 5), \text{ etc.}$$

On trouve

$$x = 7442945 \qquad \text{donnant} \qquad N = 67169.14818721.$$

CHAPITRE XVI.

Criblage.

1. Les méthodes que nous venons d'examiner, sont applicables quand il s'agit d'étudier un nombre isolé, mais il convient de les modifier quand il s'agit de l'étude d'une série de nombres compris entre certaines limites ou dans une certaine forme algébrique. Il y a entre ces deux cas, à peu près la même différence, qu'entre le travail d'un artisan faisant une œuvre d'art et la fabrication en série de cette même œuvre à l'usine.

L'artisan étudiera avec soin son œuvre, sans s'occuper de ce qui ne concerne pas directement son travail.

Le fabricant en série étudiera les procédés propres à accélérer son travail. Il tâchera de faire sortir le plus de pièces possible.

Il s'occupera peu des propriétés particulières de chacun des objets qu'il fabrique et de leur parachèvement.

Il *taylorisera* la production et cherchera à en augmenter le rendement par tous les moyens possibles.

Aussi, allons nous examiner le criblage comme une opération qui s'impose pour le travail en série, mais qui n'est pas à recommander quand il s'agit d'un nombre isolé.

2. Soit à former une table des nombres premiers inférieurs à une limite donnée, par exemple 10^7.

Si on considère les $\varphi(2.3.5.7) = \varphi(210) = 48$ nombres premiers à 210 et inférieurs à 210, on peut mettre tous nombres non divisibles par 2, 3, 5 ou 7 sous la forme $210k + i$, i étant l'un de ces 48 nombres.

Cela étant, on peut former un quadrillage composé de 48 colonnes réservées à ces 48 valeurs différentes de i et d'une colonne supplémentaire réservée à la valeur de k.

On peut même faire figurer $11.13 = 143$ lignes par page.

Alors on pourra *imprimer* une fois pour toutes, les nombres 11 et 13 dans les cases qui correspondent aux multiples de 11 et 13. Ces cases occuperont la même place sur toutes les pages, si chaque page contient 11.13 lignes.

Les tables de LEHMER [1] ne contiennent que 100 lignes par page.

On fait un criblage en inscrivant dans les tables les nombres 11, 13, 17, 19, ..., dans les cases qui correspondent à des multiples de ces nombres.

Si on continue le criblage jusqu'à la valeur de la racine carrée de la limite de la table, on éliminera tous les nombres composés. Ceux qui ne sont pas éliminés sont premiers.

3. Soit à étudier tous les nombres premiers N de la forme $k.2^n + 1$ compris entre 10^8 et 10^{12} avec $1 \leqslant k \leqslant 1000$.

Avant tout, il faut pouvoir écrire, fût-ce indirectement, les nombres à étudier.

Nous conviendrons d'écrire la valeur de n dans l'entête des colonnes et la valeur de k dans une colonne spéciale.

Les limites imposées pour N ($10^8 < N < 10^{12}$) donnent les limites suivantes de k et de n

$$n \leqslant 16, \qquad k > \frac{10^8}{2^{16}} \quad \text{ou} \quad k > \frac{5^8}{2^8} \quad \text{ou} \quad k > 1000,$$

limites incompatibles avec les limites de k imposées.

Ainsi, dans cette table ne figureront pas les expressions $k.2^n + 1$ avec $n < 17$. Il en est de même de $n \geqslant 40$.

Donc, pour que N soit compris entre 10^8 et 10^{12}, il faut que n soit compris entre 17 et 39 (si $1 \leqslant k < 1000$).

Si on désigne par k_1 et k_2 les deux limites de k correspondant à une valeur donnée de n, on trouve les résultats suivants, M désignant le nombre des nombres de la forme envisagée

$n =$	17,	18,	19,	20,	21,	22,	23,	24,	25,
$k_1 =$	765,	383,	191,	97,	49,	25,	13,	7,	3,
$k_2 =$	999,	999,	999,	999,	999,	999,	999,	999,	999,
M $=$	118,	309,	405,	452,	476,	488,	494,	497,	499,

(1) LEHMER. Factor Table. Washington 1909.

$n =$	26,	27,	28,	29,	30,	31,	32,	33,	34,	35,	36,
$k_1 =$	3,	1,	1,	1,	1,	1,	1,	1,	1,	1,	1,
$k_2 =$	999,	999,	999,	999,	931,	465,	231,	115,	57,	29,	13,
M =	499,	500,	500,	500,	466,	233,	116,	58,	29,	15,	7,

$n =$	37,	38,	39,	total,
$k_1 =$	1,	1,	1,	
$k_2 =$	7,	5,	1,	
M =	4,	2,	1,	6668.

Ces 6668 nombres sont tous impairs. On commencera par en éliminer les multiples de $p = 3, 5, 7, 11$, etc.

Pour $p = 3$, on trouvera que $N \equiv 0$ (Mod. 3), si n étant pair, $k \equiv 2$, ou pour n impair $k \equiv 1$.

Pour $p \equiv 5$, $N \equiv 0$, si

$$n \equiv 0,\ 1,\ 2,\ 3 \text{ (Mod. 4)},$$
$$k \equiv 4,\ 2,\ 1,\ 3 \text{ (Mod. 5)}.$$

On continuera ainsi à éliminer les multiples des $p = 7, 11, \ldots$, jusqu'au $p = 997$.

On peut avantageusement se servir du « A Binary Canon » de M. Cunningham [1] qui donne x et y pour toutes les valeurs de p tel que $y \equiv 2^x$ (Mod. p).

Soit, par exemple, à trouver les multiples de $p = 613$. On a

$$2^{306} \equiv -1 \quad \text{ou} \quad 2^{306-n}.2^n + 1 \equiv 0 \quad \text{d'où} \quad k = 2^{306-n}.$$

On trouve ainsi (Binary Canon, p. 72).

$n =$	17,	18,	19,	20,	21,	22,	23,	24,	25,	26,
			27,	28,	29,	30,	31,	32,	33,	34,
$306 - n =$	289,	288,	287,	286,	285,	284,	283,	282,	281,	280,
			279,	278,	277,	276,	275,	274,	273,	
$k \equiv 2^{306-n} \equiv$		287,		225,	419,		258,	129,	371,	
			246,	123,	368,	184,	92,	46,	23,	318,
ou bien $k =$							871,			
			859,		981,	797,	705,	659,		931.

(1) Cunningham. A Binary Canon. London 1900.

Certains de ces résultats sont en dehors des limites de la table par exemple $k = 287$, $n = 18$ ou $k = 931$, $n = 34$, le premier étant $< 10^8$, le second $> 10^{12}$. Il en est de même de $n \geqslant 35$.

Ceux qui y figurent sont inutilisables, si le nombre N est déjà éliminé par une valeur de $p < 613$.

Il en est ainsi des résultats

$$n = 20,\ 21,\ 23,\ 24,\ 25,\ 27,\ 30,\ 32,$$

$$k = 225,\ 419,\ 871,\ 129,\ 371,\ 859,\ 797,\ 23,$$

déjà éliminés par

$$p = 241,\ 7,\ 3,\ 5,\ 31,\ 3,\ 3,\ 3.$$

Mais on utilisera les résultats

$$n = 28,\ 29,$$

$$k = 123,\ 981,$$

pour lesquels $p = 613$ est le plus petit facteur.

4. Ayant ainsi éliminé les nombres qui ont un facteur inférieur à 1000, il restera environ 1100 nombres qui sont, ou bien premiers, ou tels que leur plus petit facteur est > 1000.

Il n'est pas nécessaire de continuer l'élimination pour $p > 1000$.

On procèdera comme suit :

On vérifiera si la congruence $2^{N-1} \equiv 1$ (Mod. N), est satisfaite.

Si la congruence en question est satisfaite, le nombre N est premier.

Il en est ainsi pour 572 nombres.

Dans presque la totalité des cas, on peut facilement étudier, si la congruence $2^x \equiv 1$ (Mod. N) est vérifiée pour sous-multiple de $\frac{N-1}{2}$. On aura ainsi des preuves positives de la primalité de N.

Il est à retenir le résultat intéressant suivant

$k = 579$, $n = 21$, $N = 1214251009$ diviseur de $F_{15} = 2^{2^{15}} + 1$.

On aura ainsi un nouveau diviseur des nombres de Fermat.

Un autre résultat de cette nature ($k = 5$, $n = 25$) est donné par PERVOUCHINE (1878) [1].

Les nombres pour lesquels la congruence $2^{N-1} \equiv 1$ (Mod. N), n'est pas vérifiée, sont composés.

On en cherchera la factorisation par les procédés exposés précédemment.

On trouvera ces résultats dans les pages qui suivent.

---

[1] Nous avons donné (T. I, p. 22) une liste des résultats connus. Nous la donnons ici une deuxième fois, en la complétant par le nouveau diviseur.

n	Facteurs de F_n	Auteurs	Date
5	$F_5 = 641 \times 6700417$	Euler	1732
6	$F_6 = 274177 \times 67280421310721$	Landry	1880
7	Composés, mais on n'en connaît pas les facteurs	Morehead, Western	1909
8			
9	$37.2^{16} + 1$	Western	1903
11	$39.2^{13} + 1$	Cunningham	1899
	$119.2^{13} + 1$		
12	$7.2^{14} + 1$	Pervouchine, Lucas	1878
	$397.2^{16} + 1$	Western	1903
	$973.2^{16} + 1$	Western	1903
15	$573.2^{21} + 1$	Kraïtchik	1925
18	$13.2^{20} + 1$	Western	1903
23	$5.2^{25} + 1$	Pervouchine	1878
36	$5.2^{39} + 1$	Seelhoff	1886
38	$3.2^{41} + 1$	Cullen, Cunningham Western	1903
73	$5.2^{75} + 1$	Morehead	1905

Voici à cette occasion une démonstration du premier résultat d'EULER que F_5 est divisible par $p = 641$.

On a

$$641 = 1 + 5.2^7 = 2^4 + 5^4,$$

ou (Mod. 641)

$$2^7 \equiv -\frac{1}{5}, \qquad \left(\frac{2}{5}\right)^4 \equiv -1.$$

La première congruence donne $2^8 \equiv -\frac{2}{5}$, et en élevant à la quatrième puissance

$$2^{32} \equiv \left(-\frac{2}{5}\right)^4 \equiv \left(\frac{2}{5}\right)^4 \equiv -1.$$

	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
1								3	17	3	5	3	641	3	5	3	17	3	5	3
3						7	13	5	7	79	—	5	19	13613	7	5	—	7	13	
5						—	3	23	3	7	3	11	3	13	3	7	3	47		
7					3907	3	—	3	11	3	29	3	113	3	379	3	166609	3		
9					5	3313	1093	443	5	11	73	3881	5	—	13	41	5			
11					3	89	3	4271	3	47	3	107	3	19	3	13	3			
13				5	7	3	2129	3	—	3	7	3	60539	3	11	3	7			
15				11	83	12253	31	—	263	13	23	17	863	11	19	113				
17				9871	3	5	3	—	3	5	3	7	3	5	3	19				
19				3	5	3	7	3	5	3	131	3	5	3	9587	3				
21				229	1109	29	5	13	103	43	5	41	23	355867	5	61				
23				5	3	11	3	5	3	—	3	5	3	61	3	5				
25			—	3	13	3	29	3	1481	3	3229	3	9677	3	33461	3				
27			—	31	7	5	—	7	31	5	7	11	157	5	35617	31397				
29			3	191	3	13709	3	—	3	31	3	1279	3	37	3	25247				
31			5	3	467	3	5	3	7	3	5	3	41	3	5					
33			—	5	17	—	7	5	—	7	461	5	7	47	37					
35			3	19	3	43	3	15259	3	1471	3	—	3	313	3					
37			—	3	131	3	—	3	23	3	60169	3	59	3	21067					
39			—	10337	5	26237	11	19	5	56873	71	—	5	541	7069					
41			5	2677	3	71	3	7	3	13	3	73	3	7	3					
43			281	3	67	3	—	3	13	3	11	3	—	3	271					
45			7	—	—	7	163	13567	7	—	109	7	503	23	7					
47			3	7	3	5	3	11	3	5	3	29	3	5	3					

53		—	3	5	3	677	3	5	3	23	3	5	3	58567	3
55		3	—	3	7	3	13	3	30809	3	7	3	—	3	17
57		3	307	23	11	5	41	1019	29	5	19501	2857	442837	5	11
59		101	3	11	3	7	3	—	3	157	3	7	3	17	
61		3	5	3	2207	3	5	3	59	3	5	3	7	3	
63		—	11	5	23	—	1303	5	87719	29	53	5	11	561199	
65		—	3	20771	3	103	3	491	3	—	3	23	3	73	
67		5	1471	3	17	3	59	3	19	3	4691	3	17	3	
69		7	59	53	5	73	—	7	5	311	7	287867	5	7	
71		11	3	—	3	977	3	—	3	139	3	11	3	188171	
73		3	7	3	—	3	97	3	7	3	—	3	—	3	
75		29	109	7	643	59	7	15137	601	7	43	131	7	101	
77		5	3	—	3	5	3	19	3	5	3	31	3	5	
79		3	593	3	5	3	23	3	5	3	13	3	5	3	
81		—	5	11	281	—	5	--	35801	19	5	101891	—	11	
83		7	3	5	3	353	3	5	3	67	3	5	3	7	
85		3	11	3	37	3	36451	3	43	3	—	3	11	3	
87		5	7	41	151	5	—	17	7	5	11	7	89	5	
89		—	3	7	3	11	3	1201	3	7	3	659	3	31	
91		3	5	3	31	3	5	3	97	3	5	3	211	3	
93		11	4229	5	1609	17	883	5	53	13	—	5	109	17	
95		—	3	127	3	45139	3	487	3	199	3	311	3	4549	
97	—	3	179	3	7	3	19	3	997	3	7	3	83	3	
99	5	449	—	97	5	19	2179	13	5	23	3323	—	5	—	

	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
101		3	—	3	4019	3	7	3	—	3	29	3	7	3	109
103		7	3	6317	3	13	3	7	3	17	3	—	3	7	3
105		71	97	67	—	41	113	11	—	19	47	13	29	31091	—
107		3	5	3	—	3	5	3	—	3	5	3	460973	3	5
109		5	3	7937	3	5	3	113	3	5	3	11	3	5	3
111		23	7	5	19	7	11	5	7	—	17	5	13	—	7
113		3	23	3	5	3	701	3	5	3	359	3	5	3	—
115		379	3	7	3	239	3	—	3	7	3	17	3	599	3
117		7	5	7309	7	47	5	7	37	11	5	—	17	7	
119		3	—	3	—	3	127	3	16061	3	11	3	167	3	
121		29	3	5	3	101	3	5	3	13	3	5	3	101573	
123		31	—	137	5	11	13	17	5	613	769	29	5	—	
125		3	7	3	11	3	—	3	7	3	41	4	179	3	
127		13	3	19	3	—	3	11	3	41	3	9043	3	13	
129		5	—	7	28057	5	7	16747	—	5	26423	107	7	5	
131		3	—	3	7	3	—	3	41	3	7	3	20147	3	
133		47	3	41	3	1531	3	13	3	6473	3	—	3	97	
135		—	13	797	1181	17	23	19	11	2131	210869	—	—	17	
137		3	5	3	449	3	5	3	—	3	5	3	11	3	
139		5	3	13	3	5	3	31	3	5	3	7	3	5	
141		—	181	5	13	19	223	5	11087	83	11	5	—	137	
143		3	41	3	5	3	7	3	5	3	1811	3	5	3	
145		7	3	2917	3	11	3	7	3	—	3	19	3	7	
147		19	5	31	11	48091	5	—	31	13	5	199	653	31	
149		3	541	3	19	3	13	3	—	3	71	3	1213	3	
151		—	3	5	3	—	3	5	3	31	3	5	3	11	
153		11	7	7823	5	7	53527	—	5	571	31	7	5	13	
155		3	73	3	—	3	11	3	17	3	—	3	—	3	
157		23	3	7	3	—	3	17	3	7	3	13	3	—	
159		5	11	—	7	5	157	7	122021	5	7	—	11	5	
161		3	13	3	9349	3	17	3	2797	3	79	3	40639	3	
163		41	3	—	3	53	3	199	3	47	3	—	3	1129	
165		107	131	13	157	3209	—	17471	1231	227	103	41	191	20899	
167		3	5	3	13	3	5	3	7	3	5	3	1997	3	
169		5	3	653	3	5	3	—	3	5	3	53	3	5	
171		17	677	5	29	—	7	5	28019	7	13	5	7	—	
173		3	43	3	5	3	2099	3	5	3	7	3	5	3	
175		11	3	53	3	79	3	109	3	23	3	11	3	—	
177		—	5	89	—	67	5	743	13	68111	5	23227	19	—	
179		3	17	3	293	3	563	3	11	3	17	3	47	3	
181		13159	3	5	3	7	3	5	3	19	3	5	3	—	
183		271	—	17	5	4021	71	1693	5	11	347	13	5	29	
185		3	—	3	17	3	7	3	47	3	11	3	7	3	
187		7	3	59	3	29	3	7	3	61	3	9439	3	7	
189		5	157	15139	61	5	67	811	17	5	163	266971	13	5	
191	—	3	29	3	11	3	3739	3	19	3	23	3	173	3	
193	3	79	3	3727	3	—	3	11	3	—	3	—	3	19	
195	1493	—	7	11	23	7	17	67	7	107	19	7	—	11	
197	—	3	5	3	163	3	5	3	463	3	5	3	67	3	
199	3	5	3	7	3	5	3	29	3	5	3	23	3	5	

	19	20	21	22	23	24	25	26	27	28	29	30	31	32
201	149	7	31	5	7	23	13	5	11	137	7	5	31	7
203	5	3	11	3	5	3	—	3	5	3	—	3	5	3
205	3	13	3	9323	3	283	3	—	3	11	3	—	3	13
207	11	853	5	19483	37	13	5	101	193	131	5	59	2833	47
209	241	3	7	3	881	3	37	3	7	3	149	3	26597	3
211	3	—	3	5	3	11	3	5	3	—	3	5	3	—
213	5	37	13	7	5	1579	7	53	5	7	17	138511	5	353
215	13	3	79	3	7	3	61	3	6163	3	7	3	13	3
217	3	43	3	11	3	19	3	23	3	503	3	17	3	11
219	43	5	—	—	13	5	—	3433	—	5	180751	11	17	5
221	787	3	—	3	1667	3	11	3	383	3	17489	3	29	3
223	3	19	3	239	3	7	3	5381	3	146023	3	7	3	43
225	—	241	11	—	19	11633	22619	17	257	13	1217	593	11	—
227	7	3	5	3	197	3	5	3	4447	3	5	3	7	3
229	3	5	3	23	3	5	3	7	3	5	3	181	3	5
231	83	13	47	5	1709	107	1381	5	—	29	176023	5	43	13
233	5	3	241	3	5	3	—	3	5	3	19	3	5	
235	3	—	3	—	3	—	3	577	3	89	3	13	3	
237	19	29	5	43	167	7	5	11	7	182111	5	7	479	
239	179	3	13	3	241	3	20749	3	53	3	—	3	—	
241	3	11	3	5	3	829	3	5	3	7	3	5	3	
243	5	7	107	13	5	—	11	7	5	79	7	193	5	
245	23	3	139	3	13	3	—	3	11	3	173	3	499	
247	3	31	3	317	3	23	3	—	3	188303	3	31	3	
249	6607	5	29	191	—	5	193	19	79	5	13	8803	23	
251	11	3	7	3	41	3	19	3	7	3	11	3	59	
253	3	5843	3	2341	3	251	3	307	3	127	3	257	3	
255	7	631	827	7	251	11	7	4373	13	7	4481	18481	7	
257	17	3	5	3	7	3	5	3	17	3	5	3	1031	
259	3	5	3	251	3	5	3	11	3	5	3	19	3	
261	1087	19	101	5	347	10141	25929	5	—	172999	—	5	139	
263	5	3	31	3	5	3	17	3	5	3	—	3	5	
265	3	499	3	853	3	7	3	5923	3	373	3	7	3	
267	13	4157	5	719	137	331	5	97	11	23	5	383	13	
269	7	3	11	3	41	3	7	3	—	3	367	3	7	
271	3	7	3	5	3	17	3	5	3	11	3	5	3	
273	5	17	19	1061	5	487	23	317	5	17	11	2473	5	
275	19	3	—	3	31	3	—	3	—	3	13	3	61	
277	3	—	3	—	3	11	3	587	3	13	3	977	3	
279	61	5	7	19	11	5	13	58657	7	5	37	7	29	
281	71	3	17	3	37	3	47903	3	13	3	17	3	33529	
283	3	13	3	7	3	2971	3	617	3	7	3	—	3	
285	41	7	—	17	7	13	79	7	—	97	7	11	50341	
287	53	3	5	3	17	3	5	3	—	3	5	3	17	
289	3	5	3	—	3	5	3	13	3	5	3	93253	3	
291	17	—	11	5	6793	—	1559	5	17	41	71	5	11	
293	5	3	7	3	5	3	43	3	5	3	47	3	5	
295	3	23	3	13	3	71	3	63103	3	19	3	—	3	
297	7	—	5	7	13	211	5	43	—	7	5	19	7	
299	137	3	97	3	7	3	331	3	43	3	7	3	43651	

	18	19	20	21	22	23	24	25	26	27	28	29	30	31
301		3	13291	3	5	3	191	3	5	3	7411	3	5	3
303		5	43	—	37	5	29	179	11	5	13	2777	—	5
305		43	3	—	3	—	3	13	3	19	3	—	3	602831
307		3	11	3	167	3	7	3	—	3	17	3	7	3
309		4783	5	—	83	199	5	11	23	3617	5	19	31	349
311		7	3	19	3	61	3	7	3	11	3	—	3	7
313		3	7	3	29	3	—	3	7	3	23	3	13	3
315		37	—	17	—	17419	607	10627	13	—	11	17	293	32303
317		11	3	5	3	179	3	5	3	29	3	5	3	43
319		3	5	3	17	3	5	3	53	3	5	3	17	3
321		431	47	7	5	17	7	82727	5	7	7481	179	5	17
323		5	3	18493	3	5	3	67	3	5	3	309929	3	5
325		3	313	3	7	3	2267	3	11	3	7	3	59	3
327		223	7	5	11	7	59	5	7	23	331	5	—	33937
329		29	3	61	3	1291	3	1181	3	—	3	23	3	19
331		3	—	3	5	3	19	3	5	3	—	3	5	3
333		5	547	2267	31	5	79	—	4073	5	19	29	43	5
335		—	3	7	3	—	3	431	3	7	3	—	3	11
337		3	19	3	21383	3	13	3	—	3	11	3	23	3
339		7	5	—	7	19	5	7	—	37	5	11	13	7
341		—	3	—	3	7	3	70039	3	829	3	7	3	23
343		3	—	3	—	3	11	3	40237	3	43	3	37	3
345		13	—	43	227	11	—	11701	37	53	1151	281	—	13
347		1301	3	5	3	—	3	5	3	—	3	5	3	569
349		3	5	3	11	3	5	3	—	3	5	3	7	3
351		19	11	1237	5	419	41	1301	5	103	47	67	5	—
353		5	3	—	3	5	3	7	3	5	3	13	3	5
355		3	7	3	19	3	—	3	7	3	13	3	29	3
357		733	4261	5	509	—	73	5	—	—	907	5	79	11
359		17	3	14717	3	59	3	643	3	13	3	7879	3	277
361		3	13	3	5	3	29	3	5	3	—	3	5	3
363		5	1741	7	433	5	7	1907	19	5	1171	—	7	5
365		—	3	29	3	2039	3	17	3	10369	3	43	3	127
367		3	823	3	7	3	3217	3	13	3	7	3	113	3
369		6337	5	13	1447	7	5	29	7	10867	5	7	7577	59
371		13	3	811	3	—	3	31	3	—	3	41	3	13
373		3	11	3	13	3	17	3	29	3	37	3	11	3
375		59	17	—	—	13	53	11	—	2203	17	23	—	37
377		127	3	5	3	19	3	5	3	7	3	5	3	151
379		3	5	3	41	3	5	3	—	3	5	3	3251	3
381		7	—	—	5	47743	37	7	5	19	7	1973	5	7
383	3	5	3	17	3	5	3	13	3	5	3	7	3	5
385	283	3	4397	3	27919	3	23	3	41	3	68113	3	197	3
387	353	29	13	5	17	4231	11	5	31	—	—	5	17	23
389	3	19	3	23	3	11	3	1697	3	149	3	487	3	17
391	5	3	—	3	5	3	7	3	5	3	—	3	5	3
393	463	5	167	—	11	5	—	—	13	5	193	7649	827	5
395	3	7	3	13	3	—	3	7	3	31	3	113	3	7
397	29	4	7	3	137	3	—	3	7	3	2333	3	—	3
399	31	8161	5	397	13	31	5	17	479	11	5	1979	151673	517207

	18	19	20	21	22	23	24	25	26	27	28	29	30	31
401	3	31	3	11	3	13	3	41	3	167	3	31	3	11
403	11	3	5651	3	2141	3	1733	3	173	3	11	3	8527	3
405	7	11	20369	7	967	503	7	1291	223	7	23	11	7	19
407	3	47	3	5	3	—	3	5	3	79	3	5	3	11437
409	—	3	5	3	7	3	5	3	101	3	5	3	14621	3
411	5	—	7	67	5	7	439	23	5	13	53	7	5	193
413	3	5	3	5399	3	5	3	—	3	5	3	223	3	5
415	53	3	47	3	11	3	13	3	—	3	59	3	—	3
417	13	—	11	5	103	193	—	5	47	59	—	5	11	5779
419	3	—	3	7	3	109	3	11	3	7	3	2551	3	137
421	5	3	101	3	5	3	—	3	5	3	1511	3	5	3
423	1481	5	191	11	7	5	—	7	347	5	7	19	401	5
425	3	277	3	19	3	7	3	439	3	—	3	7	3	—
427	487	3	—	3	—	3	179	3	39869	3	84653	3	137	3
429	17	23	5	—	29	37	5	59	17	—	5	61	23	53
431	3	211	3	43	3	—	3	37	3	569	3	13	3	41
433	7	3	23	3	1423	3	7	3	227	3	13	5	7	3
435	—	—	37	23	311	30697	3463	13	11	61	3697	39227	97	379
437	3	7	3	5	3	—	3	5	3	13	3	5	3	7
439	—	3	5	3	61	3	5	3	7	3	5	3	11	3
441	5	1619	89	—	5	43	13	11	5	2003	157733	2393	5	89
443	3	5	3	67	3	5	3	79	3	5	3	137	3	5
445	37	3	2311	3	—	3	19	3	13	3	47	3	769	3
447	7	—	—	5	37579	—	7	5	23	7	11	5	7	42901
449	3	11	3	31	3	1607	3	—	3	10711	3	11	3	13
451	5	3	19	3	5	3	—	3	5	3	7	3	5	3
453	—	5	7	—	3607	5	11	49411	7	5	36083	7	135433	5
455	3	7867	3	23189	3	11	3	2557	3	23203	3	251	3	79
457	4547	3	11257	3	31	3	43	3	11	3	—	3	87407	3
459	—	—	5	—	11	13591	5	61	107	41	5	—	13877	839
461	3	17	3	7	3	29	3	13	3	7	3	19	3	47
463	17	3	181	3	79	3	31	3	17	3	29	3	—	3
465	317	7	13	—	7	6863	139	7	349	11	7	233	71	7
467	3	—	3	5	3	7	3	5	3	47	3	5	3	
469	11	3	5	3	19	3	5	3	43	3	5	3	13	
471	5	11	—	41	5	23	509	1721	5	43	13037	11	5	
473	3	5	3	13	3	5	3	157	3	5	3	59	3	
475	7	3	43	3	83	3	7	3	—	3	137	3	7	
477	—	43	17	5	13	11	23	5	19	—	17	5	67	
479	3	7	3	—	3	13	3	7	3	1499	3	8059	3	
481	5	3	7	3	5	3	53	3	5	3	101	3	5	
483	—	5	11	—	—	5	19	41	—	5	65809	13	11	
485	3	—	3	17	3	53	3	11	3	12653	3	17	3	
487	—	3	67	3	29	3	—	3	—	3	—	3	19	
489	7	—	5	7	17	89	5	3989	29	7	5	701	7	
491	3	109	3	29287	3	17	3	—	3	29	3	—	3	
493	19	3	18077	3	7	3	13	3	23	3	7	3	41	
495	13	17	7	37	43	7	—	31	7	17	—	7	13	
497	3	—	3	5	3	41	3	5	3	107	3	5	3	
499	—	3	5	3	151	3	5	3	827	3	5	3	47	

	18	19	20	21	22	23	24	25	26	27	28	29	30
501	5	13	97	19	5	1523	521	17	5	12601	67	37	5
503	3	5	3	7	3	5	3	23	3	5	3	30211	3
505	1171	3	11	3	23	3	223	3	191	3	47497	3	11
507	1129	7	—	5	7	—	18211	5	—	2617	7	5	—
509	3	751	3	53	3	7	3	313	3	11	3	7	3
511	5	3	17	3	5	3	89381	3	5	3	13	5	5
513	11	5	1453	47	—	5	83	13	—	5	11	23	—
515	3	11	3	773	3	59863	3	101	3	13	3	11	3
517	7	3	13	3	—	3	7	3	20809	3	53	3	7
519	37	151	5	17	31	29	5	15787	—	31	5	17	617
521	3	7	3	—	3	11	3	7	3	677	3	—	3
523	31	3	7	3	17	3	23	3	7	3	19	3	17
525	9479	31	23	13	11	17	31	199	—	71	—	31	19
527	3	13	3	5	3	43	3	5	3	859	3	5	3
529	41	3	5	3	13	3	5	3	—	3	5	3	29
531	5	41	71	7	5	13	7	3539	5	7	—	121789	5
533	3	5	3	11	3	5	3	13789	3	5	3	—	3
535	11	3	103	3	7	3	29	3	—	3	7	3	64817
537	—	11	7	5	631	7	—	5	7	223	13	5	—
539	3	101	3	19	3	911	3	13	3	137	3	563	3
541	5	3	53	3	5	3	11	3	5	3	163	3	5
543	—	5	13	—	41	5	17	29	—	5	23	—	131
545	3	401	3	7	3	101	3	89	3	7	3	524257	3
547	13	3	21727	3	11	3	—	3	29	3	73	3	13
549	97	7	5	—	7	491	5	7	13	29	5	619	11
551	3	—	3	13	3	7	3	11	3	1093	3	7	3
553	107	3	293	3	—	3	—	3	19	3	61	3	—
555	—	103	—	11	13	61	997	19	43	—	197	269	173
557	3	4297	3	5	3	13	3	5	3	23	3	5	3
559	7	3	5	3	—	3	5	3	4363	3	5	3	7
561	5	29	43	2939	5	5309	131	14923	5	37	19	13	5
563	3	5	3	21613	3	5	3	7	3	5	3	271	3
565	17	3	7	3	—	3	3947	3	7	3	—	3	37
567	43	23	179	5	2543	19	—	5	11	13	149	5	23
569	3	4211	3	37	3	103	3	17	3	—	3	112331	3
571	5	3	11	3	5	3	13	3	5	3	1447	3	5
573	7	5	41	7	—	5	7	11	31	5	57349	197	7
575	3	1297	3	—	3	1289	3	16603	3	11	3	19	3
577	—	3	—	3	7	3	17	3	79	3	7	3	8123
579	11	13	5	—	1877	7	5	37	7	199	5	7	157
581	3	11	3	—	3	11491	3	61	3	31	3	11	3
583	73	3	37	3	19	3	97	3	1217	3	2287	3	—
585	31	—	29	71	101	31	11	53	23	183881	31	33857	14519
387	3	31	3	5	3	11	3	5	3	7	3	5	3
589	409	3	5	3	—	3	5	3	11	3	5	3	14321
591	5	7	1103	277	5	53	109	7	5	211	7	59	5
593	3	5	3	73	3	5	3	19	3	5	3	7	3
595	103	3	13	3	4517	3	35111	3	1063	3	37	3	359
597	—	17	61	5	23	601	13	5	67	11	—	5	438887
599	3	157	3	11	3	317	3	47	3	—	3	5653	3

	18	19	20	21	22	23	24	25	26	27	28	29	30
601	5	3	9907	3	5	3	7	3	5	3	11	3	5
603	—	5	19	13	29	5	37	17	853	5	223	11	127
605	3	7	3	263	3	19	3	7	3	1361	3	23	3
607	19	3	7	3	13	3	11	3	7	3	—	3	71
609	—	—	5	149	47	11	5	71	—	19	5	60149	283
611	3	37	3	—	3	83	3	—	3	167471	3	2003	3
613	10039	3	17	3	11	3	61	3	—	3	17	3	23
615	7	89	11	7	22037	—	7	7717	53189	7	13	169457	7
617	3	19	3	5	3	—	3	5	3	733	3	5	3
619	61	3	5	3	7	3	5	3	7459	3	5	3	31
621	5	1307	7	11	5	7	3203	82757	5	2459	1283	7	5
623	3	5	3	—	3	5	3	1621	3	5	3	29	3
625	13	3	—	3	17	3	—	3	204161	3	174289	3	13
627	53	—	109	5	—	17	92363	5	13	283	6959	5	—
629	3	—	3	7	3	173	3	119981	3	7	3	—	3
631	5	3	331	3	5	3	5471	3	5	3	673	3	5
633	17	5	127	—	7	5	—	7	11	5	7	100699	4051
635	3	3833	3	31	3	7	3	193	3	37	3	7	3
637	3947	3	11	3	—	3	1429	3	53	3	19	3	11
639	—	67	5	199	—	63587	5	11	—	—	5	13	19
641	3	—	3	30113	3	73	3	23	3	11	3	—	5
643	7	3	29	3	23	3	7	3	2111	3	3659	3	7
645	11	61	239	761	—	46919	17	5801	293	13	11	353	29
647	3	7	3	5	3	31	3	5	3	19	3	5	3
649	9467	3	5	3	—	3	5	3	7	3	5	3	103
651	5	107	4813	—	5	37	11	887	5	—	59	19	5
653	3	5	3	19	3	5	3	37	3	5	3	—	3
655	109	3	41	3	—	3	—	3	11	3	—	3	—
657	7	13	37	5	11	47	7	5	59	7	641	5	7
659	3	23	3	887	3	—	3	29	3	101	3	3359	3
661	5	3	563	3	5	3	23	3	5	3	7	3	5
663	—	5	7	113	—	5	—	95857	7	5	173	7	—
665	3	17	3	11	3	—	3	59	3	17	3	13	3
667	11	3	79	3	43	3	233	3	17	3	11	3	617051
669	4049	11	5	59	—	1039	5	13	—	—	5	11	—
671	3	—	3	7	3	—	3	17	3	7	3	—	3
673	47	3	13	3	37	3	11	3	89	3	97	3	79
675	67	7	73	—	7	11	13	7	—	313	7	73	631
677	3	29	3	5	3	7	3	5	3	2269	3	5	3
679	3671	3	5	3	11	3	5	3	13	3	5	3	59
681	5	311	11	13	5	19	47	31	5	—	17	29	5
683	3	5	3	5387	3	5	3	11	3	5	3	8467	3
685	7	3	—	3	13	3	7	3	277	3	383	3	7
687	29	1063	3823	5	18587	13	991	5	61	109	389	5	47
689	3	7	3	17	3	67	3	7	3	—	3	17	3
691	5	3	7	3	5	3	151	3	5	3	—	3	5
693	41	5	647	35141	17	5	53	47	21613	5	13	83	17
695	3	41	3	61	3	17	3	13	3	23	3	101	3
697	23	3	47	3	19	3	—	3	31	3	233	3	—
699	7	17	5	7	239	43	5	15131	11	7	5	41	7

	17	18	19	20	21	22	23	24	25	26	27	28	29	30
701		3	881	3	47	3	23	3	1723	3	139	3	--	3
703		13	3	11	3	7	3	167	3	—	3	7	3	11
705		—	23	7	1319	31	7	307	11	7	31	6917	7	23
707		3	71	3	5	3	199	3	5	3	11	3	5	3
709		31	3	5	3	823	3	5	3	8599	3	5	3	53093
711		5	31	—	23	5	149	19	—	5	107	11	31	5
713		3	5	3	7	3	5	3	83	3	5	3	11	3
715		—	3	17	3	—	3	43	3	37	3	17	3	19
717		1663	7	19	5	7	—	11	5	—	—	7	5	—
719		3	—	3	1901	3	7	3	139	3	—	3	7	3
721		5	3	223	3	5	3	71	3	5	3	20717	3	5
723		—	5	131	17	11	5	—	43	23	5	647	17	941
725		3	4637	3	12149	3	37	3	67	3	461	3	—	3
727		7	3	167	3	17	3	7	3	43	3	23	3	7
729		13	59	5	19	109	17	5	41	28621	11	5	217219	13
731		3	7	3	11	3	4801	3	7	3	41777	3	2441	3
733		11	3	7	3	—	3	—	3	7	3	11	3	61
735		17	11	—	—	19	—	61	—	17	167	181	11	—
737		3	—	3	5	3	—	3	5	3	89	3	5	3
739		43	3	5	3	173	3	5	3	151	3	5	3	41
741		5	101	103	7	5	11	7	9769	5	7	284927	229	5
743		3	5	3	—	3	5	3	31	3	5	3	13	3
745		29	3	1123	3	7	3	17597	3	13781	3	7	3	67
747		293	—	7	5	37	7	17	5	7	151	191	5	11
749		3	2903	3	—	3	8123	3	11	3	13	3	709	3
751		5	3	13	3	5	3	37	3	5	3	19	3	5
753		227	5	53	11	43	5	13	—	401	5	29	67	19
755		3	—	3	7	3	—	3	29663	3	7	3	1153	3
757		419	3	2281	3	—	3	1361	3	13	3	1051	3	328243
759		19	7	5	13	7	113	5	7	31	547	5	—	1663
761		3	13	3	127	3	7	3	1097	3	19	3	7	3
763		197	3	—	3	13	3	—	3	—	3	397	3	43
765	29	—	199	—	12011	—	13	9157	—	11	659	52543	19	56377
767	5	3	17	3	5	3	—	3	5	3	17	3	5	3
769	3	7	3	5	3	1559	3	5	3	17	3	5	3	7
771	41	5	—	149	29	5	31	283	11	5	59	13	4783	5
773	11	3	5	3	929	3	5	3	7	3	5	3	31	3
775	3	41	3	7	3	67	3	47	3	7	3	16931	3	149
777	5	11	41	13	5	29	83	97	5	1009	—	11	5	463
779	37	3	11	3	257	3	—	3	23	3	521	3	11	3
781	3	5	3	619	3	5	3	17	3	5	3	144241	3	5
783	—	7	5	17	7	5167	5	7	19	13	5	17	103	7
785	107	3	5081	3	13	3	11	3	—	3	1567	3	89	3
787	3	—	3	257	3	7	3	19	3	11	3	7	3	37
789	7	23	421	5	—	11	7	5	353	7	113	5	7	—
791	433	3	131	3	17	3	13	3	2857	3	—	3	17	3
793	3	—	3	19	3	2621	3	79159	3	47	3	463	3	89
795	11	13553	—	—	47	17	19	73	1999	41	11	71	13	17
797	5	3	23	3	5	3	17	3	5	3	7	3	5	3
799	3	11	3	5	3	227	3	5	3	—	3	5	3	133633

	17	18	19	20	21	22	23	24	25	26	27	28	29	30
801	673	5	7	23	139	5	—	43	7	5	13	7	11	5
803	7	3	5	3	23	3	5	3	—	3	5	3	7	3
805	3	—	3	31	3	61	3	11	3	103	3	37	3	31
807	5	13	19	59	5	83	11	79	5	—	131	313	5	13
809	—	3	—	3	1429	3	29	3	43	3	71	3	14251	3
811	3	5	3	—	3	5	3	7	3	5	3	29	3	5
813	9203	1361	5	11	67	179	5	269	307	43	5	—	—	11
815	19	3	7	3	—	3	137	3	7	3	43	3	53	3
817	3	—	3	7	3	107	3	1237	3	7	3	17	3	—
819	23	1283	—	5	11	—	269	5	191	19	263	5	569	29
821	13	3	43	3	31	3	1553	3	19	3	239	3	13	3
823	3	—	3	—	3	283	3	89	3	—	3	13	3	97
825	227	7	8693	79	7	71	41	7	13	383	7	—	17	7
827	5	3	—	3	5	3	21937	3	5	3	13	3	5	3
829	3	—	3	5	3	7	3	5	3	109	3	5	3	17
831	7	5	4339	7	25031	5	7	13	2237	5	—	1831	7	5
833	43	3	5	3	1013	3	5	3	29	3	5	3	230779	3
835	3	19	3	11	3	29	3	31	3	13	3	53	3	11
837	5	17	—	367	5	—	463	—	5	17	19	107	5	659
839	11	3	13	3	7	3	23	3	991	3	7	3	3677	3
841	3	5	3	61	3	5	3	—	3	5	3	269	3	5
843	101	11	5	—	19	7	5	41	7	337	5	7	—	23
845	7	3	11	3	4729	3	7	3	—	3	86477	3	7	3
847	3	—	3	23	3	—	3	67	3	—	3	77359	3	547
849	—	149	71	5	23	19	163	5	—	53	—	5	—	43
851	59	3	29	3	7457	3	11	3	13	3	947	3	191	3
853	3	7	3	907	3	—	3	7	3	11	3	—	3	7
855	—	—	11311	13	269	11	109	619	—	16673	—	271	29	61
857	5	3	7	3	5	3	127	3	5	3	37	3	5	3
859	3	13	3	5	3	—	3	5	3	7	3	5	3	13
861	11	5	757	18133	43	5	12689	839	—	5	11	316213	89431	5
863	—	3	5	3	11	3	5	3	317	3	5	3	41	3
865	3	11	3	—	3	—	3	22651	3	67	3	11	3	314569
867	5	7	11	31	5	13	29	7	5	307	7	97	5	7
869	277	3	17	3	71	3	13	3	—	3	17	3	—	3
871	3	5	3	—	3	5	3	11	3	5	3	7	3	5
873	7	19	5	7	1433	23	5	107	—	7	5	1789	7	2203
875	17	3	—	3	—	3	97	3	17	3	19	3	291089	3
877	3	83	3	—	3	11	3	149	3	41	3	—	3	29
879	—	—	—	5	3083	—	2647	5	83	251	13	5	19	11
881	29	3	7741	3	7	3	8929	3	11	3	7	3	23	3
883	3	—	3	—	3	163	3	13	3	31	3	337957	3	—
885	—	13	7	17	11	7	23	7577	7	127	751	7	—	13
887	5	3	1721	3	5	3	7	3	5	3	127	3	5	3
889	3	37	3	5	3	89	3	5	3	409	3	5	3	23
891	19	5	13	353	—	5	—	23	29	5	31	37	199	5
893	457	3	5	3	17	3	5	3	41	3	5	3	17	3
895	3	7	3	—	3	37	3	7	3	19	3	31	3	7
897	5	113	31	—	5	17	7687	31	5	11	29	—	5	17
899	13	3	7	3	211	3	17	3	7	3	1297	3	13	3

	17	18	19	20	21	22	23	24	25	26	27	28	29	30
901	3	5	3	7	3	5	3	19	3	5	3	13	3	5
903	307	—	5	137	—	3659	5	—	11	1783	5	19	25537	41
905	11	3	97	3	59	3	167	3	163	3	11	3	139	3
907	3	239	3	13	3	23431	3	62057	3	23	3	1117	3	24247
909	17	7	29	5	7	67	19	5	17	179749	7	5	—	7
911	23	3	11	3	1597	3	983	3	—	3	15427	3	11	3
913	3	—	3	—	3	7	3	1987	3	13	3	7	3	1657
915	7	—	971	7	13	—	7	11	—	7	89	47	7	59
917	5	3	13	3	5	3	11	3	5	3	—	3	5	3
919	3	29	3	5	3	13	3	5	3	11	3	5	3	823
921	7069	5	19	20089	—	5	13	499	—	5	191	1069	53	5
923	47	3	5	3	7	3	5	3	137	3	5	3	293	3
925	3	163	3	59	3	19	3	41	3	239	3	—	3	487
927	5	23	7	—	5	7	—	701	5	149	11	7	5	67169
929	7	3	—	3	11	3	7	3	13	3	317	3	7	3
931	3	5	3	—	3	5	3	—	3	5	3	11	3	5
933	61	199	5	13	53	2029	5	—	6607	19	5	277	571	
935	41	3	23	3	40699	3	—	3	19	3	67	3	283	
937	3	7	3	6037	3	79	3	7	3	37	3	71	3	
939	29	17	79	5	37	—	11	5	683	13	—	5	211	
941	1229	3	7	3	13	3	3187	3	7	3	—	3	503039	
943	3	67	3	7	3	11	3	271	3	7	3	109	3	
945	—	53	—	11	29	13	67	—	73	31	433	43	37	
947	5	3	503	3	5	3	13	3	5	3	—	3	5	
949	3	19	3	5	3	1129	3	5	3	181	3	5	3	
951	13	5	—	313	7	5	—	7	5881	5	7	1009	13	
953	31	3	5	3	—	3	5	3	397	3	5	3	1889	
955	3	47	3	491	3	7	3	1283	3	53	3	7	3	
957	5	31	113	7	5	—	7	503	5	7	13	23	5	
959	—	3	19	3	173	3	—	3	—	3	—	3	31	
961	3	5	3	—	3	5	3	13	3	5	3	797	3	
963	—	13	5	61	41	19	5	47	23	11	5	—	89	
965	8287	3	59	3	7	3	1439	3	983	3	7	3	2647	
967	3	—	3	11	3	71	3	3163	3	—	3	293	3	
969	59	281	7	5	367	7	3299	5	7	167	103	5	457	
971	7	3	17	3	33599	3	7	3	—	3	11	3	7	
973	3	17	3	1117	3	83	3	37	3	17	3	743	3	
975	—	11	443	89	353	149	173	—	41	—	421	11	138283	
977	5	3	11	3	5	3	23	3	5	3	199	3	5	
979	3	7	3	5	3	—	3	5	3	71	3	5	3	
981	10289	5	23	15991	11317	5	103	11	3	5	53	—	613	
983	109	3	5	4	47	3	5	3	7	3	5	3	863	
985	3	61	3	7	3	47	3	17	3	7	3	29	3	
987	5	19	—	17	5	11	—	13	5	29741	43	17	5	
989	53	3	—	3	2179	3	41	3	1913	3	19	3	103	
991	3	5	3	29	3	5	3	—	3	5	3	13043	3	
993	11	7	5	8377	7	20107	5	7	67	193	5	131	19	
995	337	3	13	3	11	3	311	3	145361	3	—	3	17	
997	3	11	3	—	3	7	3	—	3	69031	3	7	3	
999	7	—	11	5	—	17	7	5	509	7	—	5	7	

La table qui suit donne dans l'ordre croissant de p, la liste de 572 nombres premiers $p = k.2^n + 1$, ainsi que la plus petite solution de la congruence $2^x \equiv 1$ (Mod. p), Au lieu de la valeur de x, nous donnons celle de $j = k.2^n$: $x = \frac{p-1}{x}$.

k	n	j	k	n	j	k	n	j	k	n	j	k	n	j
191	19	4	609	18	2	235	20	2	427	20	2	823	20	8
97	20	2	39	22	6	119	21	2048	875	19	2	105	23	2
783	17	4	639	18	2	967	18	32	219	21	2	843	20	2
197	19	256	**5**(1)	**25**(1)	**10**	485	19	2	879	19	32	107	23	16
25	22	8	81	21	96	489	19	64	221	21	2	429	21	12
809	17	2	663	18	6	123	21	4	447	20	2	865	20	4
409	18	8	335	19	4	497	19	4	7	26	4	871	20	4
53	21	2	341	19	2	999	18	2	929	19	2	219	22	32
849	17	4	705	18	4	129	21	32	471	20	2	877	20	2
855	17	30	177	20	2	131	21	32	945	19	8	441	21	12
863	17	16	89	21	2	551	19	4	951	19	4	883	20	8
27	22	12	715	18	2	277	20	2	987	19	4	895	20	20
435	18	2	723	18	4	291	20	4	989	19	2	897	20	96
439	18	4	365	19	8	585	19	4	507	20	4	225	22	32
879	17	2	95	21	4	297	20	16	275	21	64	453	21	16
885	17	4	765	18	36	609	19	2	555	20	2	913	20	4
225	19	72	195	20	26	627	19	2	71	23	2	459	21	2
453	18	2	787	18	2	629	19	2	285	21	190	927	20	4
459	18	16	793	18	64	315	20	2	577	20	32	465	21	4
945	17	2	805	18	2	641	19	2	303	21	12	931	20	896
477	18	24	101	21	2	331	20	4	305	21	8	235	22	2
959	17	4	817	18	2	671	19	4	77	23	28	119	23	2
963	17	4	411	19	8	343	20	4	309	21	8	479	21	8
483	18	6	823	18	2	345	20	24	625	20	32	961	20	8
487	18	16	829	18	2	719	19	2	159	22	2	483	21	42
975	17	4	417	19	12	45	23	24	163	22	2	997	20	16
499	18	2	419	19	2	183	21	32	339	21	2	521	21	64
63	21	8	211	20	8	737	19	2	341	21	2	33	25	22
65	21	16	847	18	2	185	21	2	685	20	2	543	21	2
33	22	24	855	18	12	747	19	4	353	21	8	549	21	2
537	18	48	435	19	48	755	19	4	711	20	2	277	22	4
135	20	10	879	18	2	381	20	24	45	24	4	575	21	8
543	18	2	55	22	2	771	19	4	735	20	2	289	22	16
555	18	4	883	18	8	391	20	8	375	21	10	**579**(2)	**21**(2)	**18528**
141	20	6	447	19	6	99	22	2	381	21	6	581	21	16
577	18	2	903	18	2	795	19	12	763	20	14	73	24	2
37	22	8	913	18	2	809	19	4	765	20	2	611	21	4
597	18	6	915	18	4	819	19	14	393	21	8	155	23	8
603	18	4	459	19	18	827	19	8	795	20	64	623	21	4
151	20	2	467	19	2	837	19	2	811	20	4	315	22	4

(1) Diviseur du nombre de FERMAT F_{23}.
(2) » » » F_{15}.

k	n	j	k	n	j	k	n	j	k	n	j	k	n	j
633	21	8	347	23	2	393	24	6	449	25	8	261	27	2
651	21	4	357	23	2	397	24	2	903	24	2	525	26	96
675	21	4	715	22	10	801	23	2	931	24	98	529	26	64
343	22	8	733	22	8	203	25	2	933	24	32	535	26	2
177	23	8	371	23	8	417	24	4	945	24	30	269	27	2
735	21	12	757	22	8	421	24	2	975	24	6	543	26	8
743	21	128	765	22	36	423	24	16	491	25	4	275	27	2
749	21	2	3	30	4	219	25	584	247	26	4	285	27	2
375	22	12	193	24	4	891	23	6	991	24	2	287	27	8
789	21	4	395	23	2	451	24	2	997	24	8	145	28	4
815	21	2	407	23	4	115	26	20	129	27	16	297	27	8
51	25	6	819	22	24	927	23	72	137	27	2	609	26	4
427	22	28	13	28	8	233	25	2	149	27	8	613	26	2
27	26	768	837	22	62	935	23	16	611	25	16	315	27	4
875	21	4	847	22	2	59	27	8	307	26	2	639	26	192
445	22	32	853	22	2	951	23	8	337	26	4	329	27	2
891	21	2	859	22	8	959	23	2	339	26	4	669	26	2
903	21	14	431	23	2	487	24	4	349	26	4	675	26	96
921	21	2	865	22	8	245	25	2	711	25	2	347	27	2
953	21	2	437	23	8	987	23	2	357	26	8	703	26	4
15	27	2	879	22	2	495	24	44	45	29	2	357	27	128
483	22	4	447	23	2	33	28	2	735	25	30	717	26	2
249	23	6	915	22	2	537	24	6	375	26	10	371	27	2
999	21	2	29	27	2	547	24	4	753	25	4	763	26	64
63	25	12	939	22	64	275	25	32	379	26	2	193	28	2
127	24	16	235	24	10	553	24	8	765	25	4	387	27	12
513	22	6	957	22	2	567	24	2	785	25	16	49	30	8
517	22	4	243	24	12	71	27	2	803	25	128	799	26	4
17	27	4	979	22	2	147	26	2	415	26	2	807	26	2
553	22	2	125	25	2	153	26	4	845	25	2	823	26	2
559	22	26	507	23	2	625	24	80	849	25	16	211	28	2
565	27	4	131	25	4	633	24	2	855	25	60	847	26	1792
573	22	2	69	26	32	81	27	16	861	25	56	425	27	2
589	22	4864	291	24	4	655	24	4	869	25	4	429	27	4
37	26	4	615	23	2	663	24	416	873	25	64	477	27	2
151	24	2	617	23	2	333	25	4	219	27	2	967	26	4
305	23	160	313	24	2	169	26	64	111	28	74	975	26	960
627	22	6	659	23	4	697	24	16	911	25	2	555	27	370
157	24	2	165	25	4	723	24	4	915	25	2	35	31	10
637	22	4	665	23	38	733	24	2	921	25	8	569	27	2
639	22	12	671	23	2	23	29	16	231	27	4	9	33	48
645	22	6	345	24	40	763	24	16	475	26	2	73	30	2
81	25	8	87	26	4	393	25	48	959	25	2	599	27	16
649	22	8	355	24	4	101	27	2	483	26	12	155	29	2
655	22	4	717	23	12	205	26	2	971	25	2	39	31	12
663	22	136	735	23	6	413	25	4	487	26	2	639	27	6
669	22	6	737	23	16	837	24	8	507	26	2	651	27	2
335	23	10	755	23	10	105	27	12	513	26	2	331	28	8
171	24	6	767	23	16	841	24	8	519	26	4	669	27	4
43	26	2	779	23	64	107	27	32	65	29	2	85	30	2

k	*n*	*j*	*k*	*n*	*j*	*k*	*n*	*j*	*k*	*n*	*j*	*k*	*n*	*j*
681	27	6	495	28	12	205	30	4	653	29	2	553	30	2
689	27	2	995	27	80	825	28	6	327	30	16	583	30	2
717	27	2	999	27	32	853	28	2	671	29	2	627	30	4
719	27	2	261	29	6	877	28	2	345	30	4	157	32	2
361	28	8	525	28	2	55	32	2	701	29	8	655	30	2
93	30	2	263	29	2	897	28	48	725	29	2	663	30	2
387	28	8	531	28	2	456	29	1224	375	30	2	669	30	12
777	27	2	133	30	4	925	28	148	759	29	66	171	32	2
391	28	2	135	30	4	963	28	2	195	31	8	697	30	16
791	27	4	565	28	32	981	28	4	397	30	2	175	32	8
203	29	2	597	28	2	491	29	4	813	29	6	351	31	72
103	30	2	607	28	2	521	29	4	415	30	4	177	32	2
831	27	96	305	29	10	533	29	4	843	29	48	717	30	96
417	28	6	311	29	4	135	31	96	849	29	2	181	32	2
849	27	2	159	30	192	543	29	8	869	29	4	735	30	192
855	27	10	163	30	4	141	31	2	885	29	2	789	30	2
457	28	2	655	28	4	283	30	2	111	32	6	99	33	8
917	27	2	335	29	8	73	32	4	909	29	8	817	30	2
117	30	2	43	32	2	295	30	160	463	30	2	105	33	20
939	27	4	691	28	8	303	30	2	239	31	2	211	32	2
941	27	2	363	29	2	155	31	2	123	32	2	425	31	172
947	27	8	3	36	2	629	29	2	507	30	2	883	30	2
239	29	2	193	30	16	641	29	16	513	30	8	225	32	8
959	27	16	99	31	18	81	32	16	537	30	2	113	33	8
487	28	2	813	28	12									

APPENDICE.

Sur le triangle rectangle en nombre entier.

1. Un triangle rectangle dont les trois côtés sont des nombres rationnels sera dit *triangle de Pythagore* ou simplement *triangle rectangle.*

Si les trois côtés sont des entiers sans diviseurs communs, le triangle sera dit *primitif.*

Tout triangle est semblable à un et un seul triangle primitif.

C'est le triangle rectangle primitif que nous étudions dans ce qui suit. Les trois côtés d'un tel triangle seront désignés par x, y, z, ces nombres étant liés par la relation de PYTHAGORE

$$x^2 + y^2 = z^2. \tag{1}$$

2. Nous allons établir deux propriétés du nombre z, hypothénuse d'un triangle rectangle primitif.

a) Dans tout triangle rectangle primitif, l'hypothénuse z est impaire.

En effet, si x et y étaient tous les deux impairs, z^2 serait de la forme $8k + 2$ et z serait incommensurable. Si x et y sont tous les deux pairs, le triangle n'est pas primitif. Donc des deux nombres x et y l'un est pair, l'autre impair ; par conséquent, z^2 est impair, ainsi que z.

b) Le nombre z hypothénuse d'un triangle rectangle primitif ne contient d'autres diviseurs premiers que ceux de la forme linéaire $4k + 1$.

En effet, d'après (1) tout diviseur de z^2 (donc aussi de z) est une somme de deux carrés premiers entre eux. Ces diviseurs sont donc des nombres premiers de la forme linéaire $4k + 1$.

Ainsi, donc z est toujours de la forme linéaire $4k + 1$ premier ou composé.

Dans ce dernier cas, tout diviseur premier de z est de la forme $4k + 1$.

Pour ce qui est de x et y l'un de ces nombres est pair et l'autre est impair.

Dans ce qui suit nous supposons que x est pair

3. Problème. — Étant donné l'un des trois côtés d'un triangle primitif trouver ce triangle, c'est-à-dire, déterminer les deux autres côtés.

Nous examinerons trois cas, suivant qu'on donne l'hypothénuse ou le côté pair ou impair de l'angle droit.

Premier cas. On donne l'hypothénuse $z = p$.

Nous supposons en premier lieu que p est un nombre premier. D'après (2) le problème n'est possible que si p est de la forme $4k + 1$. Supposons donc qu'il en soit ainsi. Alors p est une somme de deux carrés. On est donc fondé de poser

$$p = a^2 + b^2.$$

Ces nombres a et b étant l'un pair et l'autre impair.

Le carré du nombre p peut aussi être mis sous la forme d'une somme de deux carrés, *d'une seule façon.*

On a

$$p^2 = (a^2 - b^2)^2 + 4a^2b^2.$$

Cette relation conduit à poser [1]

$$\left.\begin{aligned} x &= 2ab, \\ y &= a^2 - b^2, \\ z &= a^2 + b^2 = p. \end{aligned}\right\} \quad (2)$$

Si, en deuxième lieu, p n'est pas premier, on peut encore poser

$$z = p = a^2 + b^2.$$

Seulement cette décomposition ne sera pas unique.

Toutefois, à chaque décomposition de p en $p = a^2 + b^2$ correspond une seule décomposition de p^2 en

$$p^2 = (a^2 - b^2)^2 + 4a^2b^2.$$

---

[1] On a

$$y^2 = z^2 - x^2 = (z - x)(z + x).$$

Or, $z - x$ et $z + x$ sont premiers entre eux, car leur diviseur commun, s'il existait, diviserait aussi leur somme $2z$, ainsi que leur différence $2x$.

Le produit $(z - x)(z + x)$ devant être un carré parfait, on aura

$$z - x = d^2, \qquad z + x = c^2,$$

d et c étant impairs et premiers entre eux.

Si on pose $d = a - b$, $c = a + b$, on retrouve les formules (2).

La solution donnée par (2) subsiste donc, mais elle n'est pas unique.

Les valeurs de x, y et z données par (2) vérifient (1).

Inversement, *si trois nombres x, y et z forment un triangle primitif, il existe deux nombres a et b tels que les trois nombres x, y et z s'expriment en fonction de a et b par les formules* (2).

Deuxième cas. On donne le côté pair de l'angle droit, soit $x = 2k$ le côté pair donné.

Si on pose dans (2) $a = k$, $b = 1$, il vient

$$x = 2k, \qquad y = k^2 - 1, \qquad z = k^2 + 1. \tag{3}$$

Le triangle déterminé par (3) n'est primitif que si k est pair. Si on remplace k par $2l$, il vient

$$x = 4l, \qquad y = 4l^2 - 1, \qquad z = 4l^2 + 1. \tag{3bis}$$

Ce n'est évidemment pas la seule solution possible.

Ainsi, les nombres de la forme $4k + 2$ ne peuvent entrer dans la formation d'un triangle rectangle primitif.

Troisième cas. On donne le côté impair de l'angle droit $y = 2k + 1$.

Afin d'utiliser les formules (2) on posera $a^2 - b^2 = 2k + 1$, ou

$$a + b = 2k + 1, \qquad a - b = 1,$$

ou bien

$$a = k + 1, \qquad b = k,$$

ce qui donne

$$\left.\begin{aligned} x &= 2k^2 + 2k = \frac{y^2 - 1}{2}, \\ y &= 2k + 1, \\ z &= 2k^2 + 2k + 1 = \frac{y^2 + 1}{2}. \end{aligned}\right\} \tag{4}$$

On trouvera d'autres solutions si $y = 2k + 1$ n'est pas premier.

5. Nous appellerons *angle arithmétique*, l'angle α d'un triangle rectangle.

Les fonctions circulaires d'un angle arithmétique sont rationnelles.

En effet, on aura

$$\sin\alpha = \frac{x}{y}, \qquad \cos\alpha = \frac{y}{z}, \qquad \operatorname{tang}\alpha = \frac{x}{y}, \qquad \text{etc.}$$

Inversement, *si toutes les fonctions circulaires d'un angle sont rationnelles, cet angle est arithmétique.* (Pour que toutes les fonctions circulaires soient rationnelles, il suffit que le sin et le cos le soient).

Il en est en particulier, ainsi de l'angle α si $\operatorname{tang}\frac{\alpha}{2}$ est rationnel.

Si l'on pose

$$\operatorname{tang}\frac{\alpha}{2} = \frac{a}{b},$$

on trouve

$$\sin\alpha = \frac{2ab}{a^2+b^2}, \qquad \cos\alpha = \frac{a^2-b^2}{a^2+b^2}, \qquad \text{etc.},$$

l'angle α est donc l'angle arithmétique $(2ab, a^2-b^2, a^2+b^2)$.

Inversement, si α est un angle arithmétique, $\operatorname{tang}\frac{\alpha}{2}$ est rationnel.

Si on a plusieurs angles arithmétiques $\alpha_1, \alpha_2, \ldots, \alpha_n$ toute fonction linéaire à coefficients entiers de ces angles

$$\varphi = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$$

est aussi un angle arithmétique, car le sin et le cos de φ seront rationnels.

En particulier, les angles 2α, 3α, etc., sont arithmétiques.

6. Nous appellerons triangle élémentaire un triangle primitif *dont l'hypothénuse est un nombre premier.*

L'angle arithmétique de ce triangle est l'angle arithmétique élémentaire, ou simplement l'angle élémentaire.

7. Problème.— Étant donné un triangle élémentaire dont l'hypothénuse est p, trouver le triangle primitif dont l'hypothénuse est p^2, p^3, etc.

Soit

$$x_1 = 2ab, \qquad y_1 = a^2 - b^2, \qquad z_1 = a^2 + b^2 = p, \tag{5}$$

le triangle donné.

Comme

$$p^2 = (a^2+b^2)^2 = (a^2-b^2)^2 + 4a^2b^2,$$

on aura le triangle dont l'hypothénuse est p^2 en remplaçant dans les formules (2) a et b par $a^2 - b^2$ et $2ab$.

Il vient

$$\left.\begin{aligned} x_2 &= 4\,(a^2 - b^2)\,ab, \\ y_2 &= (a^2 - b^2)^2 - 4a^2b^2 = a^4 - 6a^2b^2 + b^4, \\ z_2 &= (a^2 - b^2)^2 + 4a^2b^2 = (a^2 + b^2)^2 = p^2. \end{aligned}\right\} \quad (6)$$

On trouve de même

$$p^3 = (a^2 + b^2)^3 = (a^3 - 3ab^2)^2 + (3a^2b - b^3)^2,$$

ce qui donne

$$\left.\begin{aligned} x_3 &= 2\,(a^3 - 3ab^2)(3a^2b - b^3), \\ y_3 &= (a^3 - 3ab^2)^2 - (3a^2b - b^3)^2, \\ z_3 &= (a^3 - 3ab^2)^2 + (3a^2b - b^3)^2 = (a^2 + b^2)^3 = p^3. \end{aligned}\right\} \quad (7)$$

On vérifiera facilement qu'on aura $\alpha_2 = 2\alpha_1$ et $\alpha_3 = 3\alpha_1$, etc.

On notera que le problème *admet une seule solution.*

8. Problème. — Étant donné deux triangles élémentaires dont les hypothénuses sont p_1 et p_2, trouver le triangle élémentaire dont l'hypothénuse est $p = p_1 p_2$.

Soit

$$x_1 = 2a_1b_1, \qquad y_1 = a_1^2 - b_1^2, \qquad z_1 = a_1^2 + b_1^2 = p_1,$$

$$x_2 = 2a_2b_2, \qquad y_2 = a_2^2 - b_2^2, \qquad z_2 = a_2^2 + b_2^2 = p_2^2,$$

les deux triangles donnés.

On a

$$p = p_1p_2 = (a_1^2 + b_1^2)(a_2^2 + b_2^2) = (a_1a_2 \pm b_1b_2)^2 + (a_1b_2 \mp a_2b_1)^2$$

ce qui conduit à prendre

$$\left.\begin{aligned} x &= 2\,(a_1a_2 \pm b_1b_2)(a_1b_2 \mp a_2b_1), \\ y &= (a_1a_2 \pm b_1b_2)^2 - (a_1b_2 \mp a_2b_1)^2\,, \\ z &= (a_1a_2 \pm b_1b_2)^2 + (a_1b_2 \mp a_2b_1)^2 \\ &\qquad = (a_1^2 + b_1^2)(a_2^2 + b_2^2) = p_1p_2. \end{aligned}\right\} \quad (8)$$

Soit α_1, α_2 et α les trois angles arithmétiques de ces triangles.

On trouvera que

$$\alpha = \alpha_1 \pm \alpha_2\,.$$

Ainsi, le triangle formé de deux triangles élémentaires, aura comme angle arithmétique $\alpha_1 \pm \alpha_2$.

Ou encore, deux triangles élémentaires peuvent être composés de deux façons différentes. Les angles de ces triangles seront $\alpha_1 + \alpha_2$ et $\alpha_1 - \alpha_2$.

On trouve de même que si l'hypothénuse z peut être mise sous la forme

$$z = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_n^{a_n},$$

les $p_1 p_2 \dots p_n$ étant n nombres premiers différents de la forme $4k + 1$, il existe 2^{n-1} triangles dont l'hypothénuse est z et dont les angles sont les $n - 1$ valeurs différentes de la fonction linéaire

$$\varphi = a_1 \alpha_1 \pm a_2 \alpha_2 \pm a_3 \alpha_3 \dots \pm a_n \alpha_n,$$

$\alpha_1, \alpha_2, \dots, \alpha_n$ étant les angles de n triangles élémentaires.

9. Voici une petite table des triangles primitifs (élémentaires et composés) dont l'hypothénuse est inférieure à 1000.

Ils sont classés d'après la valeur de l'hypothénuse.

TRIANGLES ÉLÉMENTAIRES.

x	y	z	x	y	z	x	y	z	x	y	z
4	3	5	28	195	197	408	145	433	660	259	709
12	5	13	60	221	229	280	351	449	108	725	733
8	15	17	208	105	233	168	425	457	468	595	757
20	21	29	120	209	241	380	261	461	760	39	761
12	35	37	32	255	257	220	459	509	600	481	769
40	9	41	260	69	269	440	279	521	748	195	773
28	45	53	252	115	277	420	341	541	572	555	797
60	11	61	160	231	281	532	165	557	280	759	809
48	55	73	68	285	293	520	231	569	700	429	821
80	39	89	312	25	313	48	575	577	540	629	829
72	65	97	308	75	317	368	465	593	828	205	853
20	99	101	288	175	337	240	551	601	232	825	857
60	91	109	180	299	349	612	35	613	348	805	877
112	15	113	272	225	353	608	105	617	800	369	881
88	105	137	252	275	373	200	609	641	920	129	929
140	51	149	340	189	389	572	315	653	912	215	937
132	85	157	228	325	397	300	589	661	580	741	941
52	165	173	40	399	401	552	385	673	728	615	953
180	19	181	120	391	409	52	675	677	248	945	977
168	95	193	420	29	421	260	651	701	372	925	997

TRIANGLES COMPOSÉS.

x	y	z	x	y	z	x	y	z	x	y	z
24	7	25	36	323	325	184	513	545	840	41	541
			204	253		544	33				
16	63	65	76	357	365	276	493	565	116	837	845
56	33		364	27		396	403		836	123	
36	77	85	152	345	377	336	527	625	504	703	865
84	13		352	135					816	287	
44	117	125	304	297	425	100	621	629	60	899	901
			416	87		460	429		780	451	
24	143	145	84	437	445	156	667	685	464	777	905
144	17		396	203		684	37		616	663	
120	119	169									
104	153	185	360	319	481	400	561	689	924	43	925
176	57		480	31		680	111		756	533	
84	187	205	44	483	485	528	455	697	420	851	949
156	133		476	93		672	185		900	301	
140	171	221	132	475	493	364	627	725	124	957	965
220	21		468	155		644	333		884	387	
96	247	265	336	377	505	216	713	745	696	697	985
264	23		456	217		624	407		864	473	
240	161	289	92	525	533	56	783	785			
			308	435		736	273				
136	273	305				168	775	793			
224	209					432	665				

APPLICATION.

Triangle arithmétique (héronien).

10. Définition. — Un triangle sera dit arithmétique (ou héronien) si la surface et les côtés sont rationnels.

Ainsi le triangle (13, 14, 15) est arithmétique de surface $S = 84$.

11. Théorème. — Dans un triangle arithmétique, les hauteurs, le diamètre (rayon) du cercle circonscrit, les rayons des cercles tritangents, sont rationnels et les angles sont arithmétiques.

En effet, soient x, y, z, X, Y, Z, S, h_x, h_y, h_z, R, r, r_x, r_y, r_z les côtés, les angles, surface, hauteurs, rayons des cercles circonscrit et tritangents, on a

$$2S = xy \sin Z = yz \sin X = zx \sin Y = xh_x = yh_y = zh_z ,$$

$$4RS = xyz, \qquad S = pr = (p - x)\, r_x = (p - y)\, r_y = (p - z)\, r_z ,$$

étant posé $2p = x + y + z$.

Toutes ces relations sont rationnelles et si tous les éléments, sauf un, sont rationnels, l'élément excepté l'est aussi.

12. Théorème. — Tout triangle rectangle est arithmétique.

Dans le triangle $(2ab,\ a^2 - b^2,\ a^2 + b^2)$, on trouve

$$S = ab\,(a^2 - b^2).$$

On trouve encore

$$h_z = \frac{2ab\,(a^2 - b^2)}{a^2 + b^2}, \qquad h_y = 2ab, \qquad h_x = a^2 - b^2,$$

$$R = \frac{a^2 + b^2}{2}, \qquad r = b\,(a - b), \qquad r_x = b\,(a + b), \qquad r_y = a\,(a - b),$$

$$r_z = a\,(a + b).$$

La réciproque n'est évidemment pas vraie.

13. Un triangle arithmétique ne peut pas être équilatéral, car $\frac{\pi}{3}$ n'est pas un angle arithmétique.

Le triangle sera isocèle si on fait

$$\sin X = \sin Y = \frac{2ab}{a^2 + b^2} \qquad \text{ou} \qquad \frac{a^2 - b^2}{a^2 + b^2}.$$

On formera ainsi deux triangles isocèles dont les côtés sont

$$2\,(a^2 - b^2), \qquad a^2 + b^2, \qquad a^2 + b^2,$$

ou

$$4ab, \qquad a^2 + b^2, \qquad a^2 + b^2.$$

Ces deux triangles ont la même surface $2ab\,(a^2 - b^2)$.

14. Le triangle sera quelconque si on y fait intervenir deux angles arithmétiques. Puisqu'on peut prendre

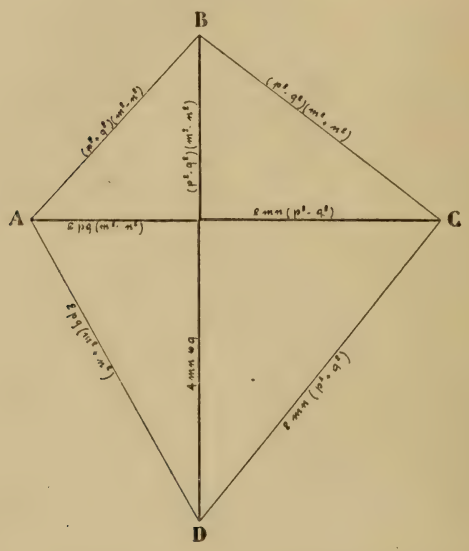
$$\sin X = \frac{2mn}{m^2 + n^2} \qquad \text{ou} \qquad \frac{m^2 - n^2}{m^2 + n^2},$$

$$\sin Y = \frac{2pq}{p^2 + q^2} \qquad \text{ou} \qquad \frac{p^2 - q^2}{p^2 + q^2},$$

on peut former quatre triangles constitués par six droites différentes.

Ces quatre triangles forment un quadrilatère inscriptible, dont les diagonales sont perpendiculaires. Le diamètre du cercle circonscrit est

$$2R = (m^2 + n^2)(p^2 + q^2).$$



Soit ABCD ce quadrilatère, et O l'intersection des diagonales, on trouve

$$BC = (m^2 + n^2)(p^2 - q^2), \qquad AB = (m^2 - n^2)(p^2 + q^2).$$

$$AD = 2pq\,(m^2 + n^2), \qquad CD = 2mn\,(p^2 + q^2),$$

$$AO = 2pq\,(m^2 - n^2), \qquad OB = (m^2 - n^2)(p^2 - q^2),$$

$$OC = 2mn\,(p^2 - q^2), \qquad OD = 4mnpq.$$

INDEX ALPHABÉTIQUE.

Les numéros inscrits sont ceux des pages correspondantes.

Les noms d'auteurs sont imprimés en italique.

	Pages.
Angle arithmétique	238
Caractères	117
Caractéristique (équation)	93
Cas d'impossibilité	76
Centre	19
Congruence caractéristique	25
Conique	19
Criblage	217
Cunningham	219, 221
Cullen	221
Cycle	195
» dérivé	195
» primitif	195
De la Vallée Poussin	IV, 198
Demoulin	IV
Dernier point entier	198
Domaine fondamental	107
Ellipse	20, 85, 209
Euclide	31
Euler	11, 119, 221
Équation d'une conique	19
» de Pell	72, 209
» caractéristique	93
Fermat	133, 134, 139, 143, 220, 233
Fibonacci	3
Formes	87
Formes binaires	87
» binomes	87, 116
» définies	95
» équivalentes	91
» indéfinies	108
» linéaires de x (Table des)	156
» primitive	92
» (Classe de)	91
Formules de récurrence	77
Fractions continues	1
» » générales	32
» » périodiques	11
» » symétriques	7
Fraction irréductible	7
Gauss	III, 119, 182
Genre	115
Héronien (triangle)	242
Hyperbole	24
» équilatère	209
Jacobi	124
» (Résidu de)	124
» (Symbole de)	124
Lagrange	11
Legendre	124
» (Résidu de)	124
» (Symbole de)	124

Pages.
Landry 135, 221
Lehmer 218
Lucas. . . . 135, 139, 140, 142, 221
Morehead 135, 221
Maret Blanc. 142
Numeri idonei. 119
Parabole 21
Pell (Équation de). . . . 72, 85, 209
Période des quotients complets. 16
Période des quotients incomplets 14, 30, 61
» toujours possible . . 58
Pervouchine 221
Point entier (dernier) . . . 198
Points entiers 19
Pomey 134
Preuve directe de primalité . . 133
Quotients incomplets. . . . 1
Récurrence (Formule de) . . 77
Réduction 26
» des formes définies . 95
» » indéfinies. 109
Réduites. 2
» (Calcul des). . . . 2
» (Propriété des). . . 3
» (Formes) 95
Réprésentation primitive . . 88
» géométrique . 105

Pages.
Résidu 121
» d'un nombre composé. 123
» jacobien 124
» de Legendre . . . 124
Résidus (Recherche des) . . 125
Seelhof 234, 135, 221
Solution dérivée 179
» directe 180
» primitive 179
Substitution automorphe . . 90
« identique . . . 90
» linéaire 98
» modulaire . . . 21, 90
» (Produit de deux) . 89
Symbole de Jacobi 124
« Legendre . . . 124
Table des formes linéaires de x. 156
Tchebicheff 177
Triangle. 235
» arithmétique . . . 240
» de Pythagore . . . 235
» élémentaire. . . . 238
» héronien 242
» primitif 235
» rectangle 235
Western 135, 221

TABLE DES MATIÈRES.

AVANT-PROPOS III

PREMIÈRE PARTIE.

Équations indéterminées du second degré à deux inconnues.

Pages.

CHAPITRE PREMIER. — **Des fractions continues** 1-18
1. Définitions. 1
2. Calcul des réduites 2
3. Propriétés des réduites. 3
4. Inégalités concernant les réduites 4
5. La différence entre une réduite et la valeur de la fraction continue. 5
6. Fraction irréductible comprise entre deux réduites 7
7. Fraction continue symétrique 7
8. Deux irrationnelles terminées par les mêmes quotients complets. 8
9. Nombre algébrique du second degré 9
10. Son développement en fraction continue 11
11. Fraction continue périodique. 12
12. Propriété des périodes 14
13. Cas particulier 15
14. Propriété des quotients complets 16
15. Propriété du développement de $\sqrt{N}$ 17
16. Racine de l'équation $x^2 + x - A = 0$ 18

CHAPITRE II. — **Équation indéterminée du second degré à deux inconnues** 19-29
1. Généralités 19
2. Cas de l'ellipse 20
3. Cas de la parabole 21
4. Cas particulier du genre hyperbole 24
5. Réduction du cas général. 25
6. Forme spéciale de l'équation d'une hyperbole 26
7. Cas où le coefficient de xy est pair 26
8. Cas où ce coefficient est impair 27
9. Cas particulier 28

CHAPITRE III. — **Développement en fraction continue de la racine positive de l'équation** $x^2 = A$ 30-60
1. Propriété de ce développement 30
2. Réciproque du théorème précédent 30
3. Cas où la période est constituée par le seul terme irrégulier . 31
4. Cas où la période est constituée de 1 terme dans la partie symétrique. 31
5. » » 2 » » 33
6. » » 3 » » 34
7. » » 4 » » 37
8. » » 5 » » 39
9. » » 6 » » 42

Pages.
10. Cas général 43
11. Périodes contenant 7 termes dans la partie symétrique . . . 45
12. » 8 » » » . . . 48
13. » 9 » » » . . . 48
14. » 10 » » » . . . 50
15. » 11 » » » . . . 50
16. » 12 » » » . . . 51
17. » 13 » » » . . . 52
18. » 14 » » » . . . 52
19. » 15 » » » . . . 53
20. » 16 » » » . . . 53
21. Période contenant plus de 16 termes dans la partie symétrique . 54
22. Cas d'impossibilité 57
23. Cas toujours possible 58
24. Théorème d'existence 60

CHAPITRE IV. — **Développement en fraction continue de la racine positive de l'équation $x^2 + x - A = 0$** 61-70
1. Propriétés de ce développement 61
2. Réciproque du théorème précédent. 62
3. Cas d'une période constituée par le terme irrégulier 62
4. Période contenant 1 terme dans la partie symétrique. . . . 63
5. » 2 » » » . . . 64
6. » 3 » » » . . . 65
6-9. Quelques développements 68
10. Cas d'impossibilité 70

CHAPITRE V. — **Équations réduites du second degré du genre hyperbole, ou équation de Pell** 72-86
1. Généralités 72
2. Solution de l'équation de Pell 73
3. Réciproque 74
4. Le signe du second membre 75
5. Cas d'impossibilité 76
6. Formules de récurrence 77
7. Autres formules 78
8. Valeurs négatives de n 79
9. Cas de l'équation $y^2 + xy - Ax^2 = \pm 1$ 81
10. Cas de l'équation générale 83
11. Équation $x^2 - Ay^2 = \pm D$ ($D^2 < A$) 85

DEUXIÈME PARTIE.

L'Arithmétique des formes quadratiques.

CHAPITRE VI. — **Généralités sur les formes** 87-94
1. Définitions 87
2. Substitutions 88
3. Produit de deux substitutions 89
4. Substitutions inverse et modulaire 90
5. Théorème sur la représentation d'un nombre N par une forme . 91

Pages.
6. Solution d'une certaine congruence 92
7. Conditions d'une représentation 92
8. Equation caractéristique 93
9. Représentation d'un entier 93
CHAPITRE VII. — **Formes quadratiques définies** 95-107
1. Définitions 95
2. Réduction d'une forme 95
3. Propriété d'une forme réduite 96
4. Deux formes réduites ne peuvent être de la même classe sans être identiques 96
5. Déterminer si deux formes réduites sont de la même classe . . . 99
6. Substitution automorphe 101
7. Cas d'une forme primitive 103
8. Cas d'un déterminant donné 104
9. Représentation géométrique 105
CHAPITRE VIII. — **Formes quadratiques indéfinies** 108-112
1. Généralités 108
2. Formes réduites 108
3. Réduction d'une forme 109
4. Nombre des formes réduites 109
5. Substitutions automorphes 110
6. Cas d'un déterminant donné 111
CHAPITRE IX. — **Formes quadratiques binaires, binomes définies** 113-120
1. Généralités 113
2. Formes ayant un même déterminant 113
3. Distinctions entre ces formes 114
4. Caractères 115
5. Formes binomes 116
6. Cas d'une seule classe par genre. Numeri Idonei 119

TROISIÈME PARTIE.

Factorisation.

CHAPITRE X. — **Les résidus quadratiques** 121-132
1. Définitions 121
2. Théorèmes sur les résidus 122
3. Semi résidu 123
4. Résidus d'un nombre composé 123
5. Symbole de Jacobi 124
6. Distinction entre le symbole de Jacobi et celui de Legendre . 124
7. Résidu d'un nombre réprésenté par une forme 124
8. Détermination des résidus d'un nombre 125
9. La représentation $N = x^2 \pm R$ 125
10-12. Mis sous la forme $N = x^2 \pm Dy^2$ 125
13. Détermination directe d'un résidu 128
14. Cas de deux facteurs 129
15. Condition pour qu'un nombre N ne contienne pas plus de deux facteurs 131

Pages.
CHAPITRE XI. — **Preuves directes de primalité** 133-143
1. Utilité de ces preuves 133
2. La réciproque du théorème de FERMAT 133
3. Autre énoncé. 134
4-5. Comparaison de ces énoncés 134
6-10. Résolution de la congruence $a^x \equiv 1$ (Mod. N) 136
11. Séries de LUCAS 139
12. Application à $N = 2^n + 1$ 140
13. » $N = 2^n - 1$ 141
14. » $N = k.2^n \pm 1$ 142
CHAPITRE XII. — **De l'équation** $x^2 - y^2 = N$.
I. **Formes linéaires de** x 144-174
1. Généralités 144
2. Nombre de solutions 144
3. Cas du module p^2 146
4. Autre méthode 147
5. Cas de $\left(\frac{N}{p}\right) = +1$ et $p \equiv 3$ (Mod. 4) 149
6. » » » 1 » 151
7. Cas de $p = 3$ et 5 153
TABLE DES SOLUTIONS 156-166
8. Répartition 166
9. Cas spécial 167
10. Cas du module 2^n 168
11. Cas de $N \equiv 1$ (Mod. 8). 169
12. Cas où -1 ou ± 2 sont résidus de N 170
13. Cas spécial 172
14. Cas de deux facteurs 173
CHAPITRE XIII. — **De l'équation** $x^2 + Dy^2 = N$ 175-194
1. Généralités 175
2. Inconnue à déterminer. 175
3. Limites des inconnues. 176
4. De l'équation $x^2 - Dy^2 = \pm N$ 176
5. » $x^2 - Dy^2 = +N$ 177
6. » $x^2 - Dy^2 = -N$ 178
7. Solutions primitives et dérivées. 178
8. L'équation $x^2 + y^2 = N$ 179
9. Solution directe 180
10. Formes linéaires de x 185
11. Cas de $\left(\frac{N}{p}\right) = +1$ 186
12-18. Module 2^n 186
19. Modules impairs 191
20-21. Cas où p divise D 192
CHAPITRE XIV. — **Des cycles**. 195-208
1. Définitions 195
2. Cas spécial 196
3. Exemples 196
4. Différentes façons de former un cycle 197

Pages.
5. Théorème sur les cycles 198
6. Cycle à former 199
7. Cycle primitif 199
8. Cycle dérivé, exemples 199
9. Cas de deux formes à déterminant négatif 206
10. » » » positif 206
11. Cas d'un cycle primitif 207
12. Substitution d'une solution à sa dérivée 207
13. Cas défavorable 208
CHAPITRE XV. — **De l'équation** $x^2 - y^2 = N$.
II. **Limites de** x **et** y **et applications** 209-216
1. Généralités 209
2. Cas d'impossibilité. Cas général 209
3. Limites de x et y 210
4. Facteur auxiliaire 211
5. Applications 213
CHAPITRE XVI. — **Criblage** 217-235
1. Cas d'application 217
2. Exemple 217
3. Nombres premiers de la forme $k.2^n + 1$ 218
4. Recherche des diviseurs de ces nombres 220

APPENDICE.

Triangle rectangle et ses applications 236-244

UNIVERSITAS SCIENTIAE OTTAVIENSIS

BRUXELLES. — IMPR. STEVENS, RUE DES FORTIFICATIONS, 9.

IMPRIMERIE
STEVENS FRÈRES
BRUXELLES

12

LA BIBLIOTHÈQUE
Faculté des Sciences
UNIVERSITÉ D'OTTAWA
Echéance

Celui qui rapporte un volume après la dernière date timbrée ci-dessous devra payer une amende de cinq sous, plus un sou pour chaque jour de retard.

THE LIBRARY
Faculty of Science
UNIVERSITY of OTTAWA
Date due

For failure to return a book on or before the last date stamped below there will be a fine of five cents, and an extra charge of one cent for each additional day.

9 JUL 1962 C

~~NOV 0 1 1977~~

~~MAY 1 2 1980~~

(CE)

a39003 006860026b

G. E. STECHERT & Co
(ALFRED HAFNER)
NEW YORK

U D' / OF OTTAWA
COLL ROW MODULE SHELF BOX POS C
333 14 05 04 16 14 4